Thecus

VisoGuard 4.0

User Manual

Thecus VisoGuard 4.0 User Manual

Document version V2 (Release 4.0.1)

Published in May 2011

The software described in this manual is licensed under the terms of the Thecus end user license agreement and may only be used in accordance with these terms.

Copyright

Copyright © 2003-2011 NETAVIS Software GmbH. All rights reserved.
Thecus and VisoGuard are trademarks of Thecus Technology Corporation. All other trademarks are trademarks of their respective holders.

Thecus Technology Corporation
15F., No.79, Sec. 1, Sintai 5th Rd., Sijhih City
Taipei County, Taiwan R.O.C.

Tel +886 (2) 2698 1788
Fax +886 (2) 2698 9098
info@thecus.com
www.thecus.com

Contents

1 Introduction 5

1.1 The VisoGuard documentation set 5
1.2 What is new with this release 5
1.3 VisoGuard data security 5
1.4 Video streaming methods and compression 6

2 Starting and operating the VisoGuard client 10

2.1 Introduction the VisoGuard client 10
2.2 Starting the VisoGuard client in a standard web browser 11
2.3 Working with the installed VisoGuard client 14
2.4 Client multi-window and multi-screen operation 17
2.5 VisoGuard Transcoding™ for low-bandwidth client-server connections 19
2.6 Exiting the client 19

3 Setting up cameras 20

3.1 Preparations 20
3.2 Adding a new camera and setting basic properties 20
3.3 Setting up the camera recording archive 26
3.4 Optional: Configuring video analytics (iCAT) 26
3.5 Defining brightness, contrast, and saturation 26
3.6 Working with camera groups 27
3.7 Changing the port mapping of analog cameras 28

4 Managing users 29

4.1 Creating a new user account 29
4.2 Setting general user privileges 30
4.3 Setting camera access rights 31
4.4 Working with user groups 31
4.5 Defining Online Monitor views for a new user 31
4.6 Information about logged-in users 32
4.7 Changing the password 32
4.8 Working with users from Active Directory or LDAP 32

5 Using the Online monitor 34

5.1 Creating a new view 34
5.2 Selecting cameras 35
5.3 Navigating in the Online monitor 36
5.4 Modifying view port settings 37
5.5 Zooming in a view port and in archive recordings 38
5.6 Manual recording control in the Online Monitor 39
5.7 Working with round tours (the Smart guard™ function) 40
5.8 Copying views between users 41
5.9 Working with MPEG cameras and audio (MPEG-4, H.264, and MxPEG) 41

6 Working with archive recordings 43

6.1 Programming archive recordings 43
6.2 Playback of archive recordings 46
6.3 Exporting recordings (images and video sequences) 52
6.4 Motion detection in archive recordings 53

7 Working with simple motion detection 56

7.1 VisoGuard's own server-based motion detection 56
7.2 Motion detection in archive recordings 59

7.3 In-camera motion detection 59

8 Handling events 61

8.1 Event list and event details 61
8.2 Searching in the event database 63
8.3 Generating an event statistics report 64

9 Working with PTZ cameras 66

9.1 Setting up a PTZ camera 66
9.2 Defining fixed PTZ positions 66
9.3 Defining PTZ routes 66
9.4 Controlling PTZ cameras 67

10 Administrating VisoGuard servers 72

10.1 Server system information and restarting 72
10.2 Setting VisoGuard server parameters 75

11 Working with interconnected VisoGuard servers 79

11.1 Adding and defining a remote VisoGuard server 79
11.2 Working with cameras of another server 80
11.3 Working with events of remote servers 82
11.4 Monitoring remote servers 82
11.5 Distributed upgrades 82

12 VisoGuard on mobile devices 83

12.1 Supported devices 83
12.2 Installing the VisoGuard client on a mobile device 83
12.3 Running the VisoGuard client on a mobile device 83

13 Working with Layout Navigation 84

13.1 Basic concepts and how it works 84
13.2 Installing the layout navigation tool 84
13.3 Starting the layout navigation tool 84
13.4 Setting up a project and defining layouts (Editing mode) 85
13.5 Customizing the behavior and appearance of controls 88
13.6 Layout navigation and operation (Navigation mode) 92

14 Video analytics with iCAT 96

14.1 iCAT highlights 96
14.2 Basic iCAT concepts 97
14.3 Setting up a camera for video analytics with iCAT 99
14.4 Working with iCAT 113

15 Special functions 117

15.1 Video annotations 117
15.2 Embedding VisoGuard video streams in web pages 117

16 Index 118

1 Introduction

Thank you for choosing Thecus VisoGuard 4.0 as the management software for your video monitoring system. As you use it, you will find that VisoGuard not only enables you to view live images and record them, but also provides a full-scale platform for the intelligent utilization of your video data.

This User Manual guides you through the functionality of Thecus VisoGuard 4.0.

If you have questions that are not answered in the VisoGuard documentation set, please contact your Thecus distribution partner, or our product management team directly by e-mail or telephone +886 (2) 2698 1788.

We wish you an interesting and productive experience with Thecus VisoGuard 4.0.

Your Thecus Team.

1.1 The VisoGuard documentation set

These documents are available:

- *Thecus VisoGuard 4.0 User Manual*
- *Thecus VisoGuard 4.0 Supported Video Sources*
- *Thecus VisoGuard 4.0 Server Installation and Administration*
- *Thecus VisoGuard 4.0 Server and Client Compatibility*
- *Thecus VisoGuard 4.0 SNAP XML Interface*

These documents are available online as PDFs directly on each VisoGuard server via the standard web interface and also from each client via the **Info** menu at the lower right corner.

1.2 What is new with this release

The changes of a release are documented in the **Release Notes**, which you can find on the standard web interface of each VisoGuard server and also under the following direct link:

http://<your-server>/relnotes

or on the public demo server

showroom.netavis.net/relnotes

There you also find the release information of previous releases.

1.3 VisoGuard data security

VisoGuard has been designed to provide the highest level of robustness and data security. The following aspects of the VisoGuard system document that:

- All video and configuration data on an VisoGuard server are stored in separate file system partitions, protected by multiple levels of security.
- Optionally the video data can be stored using 128 bit AES encryption (new since release 4.0)
- Optionally HTTPS can be used for streaming video data between cameras and servers (new since release 4.0).
- In any case, the authentication data (user names and passwords) transferred between clients and servers are encrypted by MD5 strong encryption.

Please note: Encrypting and decryption can mean higher CPU overhead at the server and/or the client. Also doing something with the contents of an encrypted stream means decryption and therefore higher CPU overhead. For example, doing video analytics with an encrypted video stream means that is has to be decrypted at the server before processing. Likewise, storing an unencrypted stream in an encrypted video database means that it has to be encrypted at the server before storing . Likewise, displaying an encrypted video stream at the client means more CPU overhead at the client because it has to be decrypted.
On the other hand, simply storing an already encrypted video stream coming from the camera does not need more CPU at the server than storing an unencrypted video stream.

1.4 Video streaming methods and compression

VisoGuard supports video streaming in several standards:

- Motion JPEG (often also referred to as MJPEG)
- MPEG-4 streaming
- H.264 streaming (also known as MPEG-4/AVC)
- MxPEG streaming (this is a streaming standard specially developed by www.mobotix.com for their IP cameras)

The big difference between the various streaming methods is the way how the image data are compressed and transferred. The selected streaming method has great influence on:

- the **bandwidth** needed for transmission between cameras and server but also between servers and clients,
- the **CPU load** at the server and the client induced by compression and decompression, and
- the **storage requirements** for recording

For low-bandwidth client-server connections VisoGuard offers the unique Transcoding™ feature (see *2.5 VisoGuard Transcoding™ for low-bandwidth client-server connections* on page 19).

1.4.1 Multi streaming (multiple parallel video streams from the camera)

Some cameras are capable of providing multiple parallel video streams to VisoGuard. This can be helpful, for example, when online viewing and recording is to be done in different formats (e.g. different sizes and frame rates) or for optimizing iCAT video analytics performance (see *14.2.1 Considerations for setting up a system with iCAT* on page 97).

Usually MJPEG cameras can deliver several MJPEG streams while MPEG cameras (MPEG-4, H.264, and MxPEG) usually can deliver only 1 or 2 MPEG streams and some camera types can deliver several MJPEG streams in addition to the MPEG stream(s).

However there are a few important restrictions with multi streaming:

- Some cameras have performance limitations in providing multiple streams depending on the streaming format, resolution, and frame rate. We found out that some cameras just stop streaming when the streaming processors of the camera get overloaded by certain resolution and frame rates settings. Please refer to the camera data sheet and documentation.
- In the current version VisoGuard supports 1 format setting for MPEG streams (MPEG-4, H.264, and MxPEG) and multiple format settings for MJPEG streams.

Please note: Please refer to camera data sheet and documentation for camera limitations. Also the document *Thecus VisoGuard 4.0 Supported Video Sources* may provide further details on camera restrictions.

1.4.2 Motion JPEG

A network camera captures individual images and compresses them into a JPEG format. The network camera can capture and compress, for example, 30 such individual images per second (30 fps), and then make them available as a continuous flow of images over a network to an VisoGuard server which then distributes it to VisoGuard clients and / or stores it in the camera archive. At a frame rate of about 16 fps and above, the viewer will perceive full motion video.

As each individual image is a complete JPEG compressed image, they will all have the same guaranteed quality, determined by the compression level as defined for the network camera or network video server.

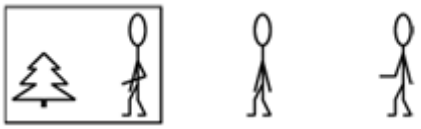
Example of a sequence of three complete JPEG images:

1.4.3 MPEG (MPEG-4, H.264, and MxPEG)

Some of the best-known audio and video streaming techniques are defined by the so called MPEG consortium (Moving Pictures Expert Group). Under the MPEG umbrella several streaming methods are available like MPEG-4, H.264, and MxPEG (strictly taken, MxPEG is not part of the standards defined by the MPEG group but is a proprietary standard by the company Mobotix. However, because of reasons of simplicity we refer to MxPEG also as an MPEG format). MPEG-4 and H.264 are well known and widely supported MPEG streaming standards.

Simply described, MPEG's basic principle is to compare two compressed images to be transmitted over the network, and using the first compressed image as a reference image (called an I-frame), only sending the parts of following images (B- and P-frames) that differ from the reference image. A viewing client will then reconstruct all images based on the reference image and the "difference data".

At the cost of higher complexity, the result of applying MPEG video compression is that the amount of data transmitted across the network is less than that of Motion JPEG. This is illustrated below where only information about the differences in the second and third frames is transmitted



H.264 and MxPEG all work very similar to MPEG-4 whereby H.264, for example, needs only about 60% of the bandwidth of MPEG-4 for roughly the same video quality. However, this efficiency does not come for free. Encoding and decoding H.264 needs more CPU power than MPEG-4. A general rule is that the higher the compression factor the heavier the CPU burden (in the server and in the clients). Therefore there is always a tradeoff between bandwidth utilization and CPU power needed.

1.4.4 Advantages and disadvantages of Motion JPEG and MPEG (MPEG-4, H.264, and MxPEG)

Due to its simplicity, Motion JPEG (MJPEG) is a good choice for use in many applications. JPEG is a widely available standard in many systems often by default. It's a simple compression/decompression technique, which means the cost, in both system time and money, for encoding and decoding is kept low. The time aspect means that there is limited delay between image capturing in a camera, encoding, transfer over the network, decoding, and finally display at the viewing station. In other words, MJPEG provides low latency due to its simplicity (image compression and complete individual images), and for this reason it's also well suited for when image processing is to be performed, for example video motion detection or object tracking.

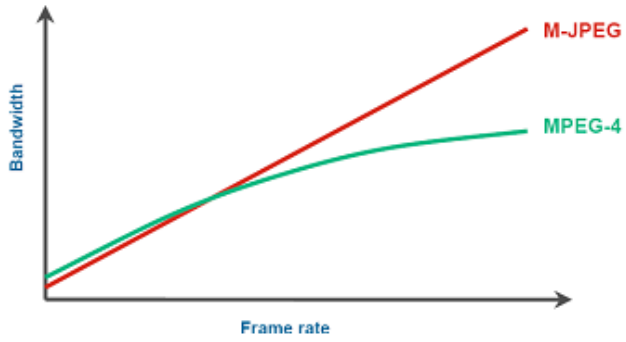
MJPEG gives a guaranteed image quality regardless of movement or complexity of the image scenes. It still offers the flexibility to select either high image quality (low compression) or lower image quality (high compression) with the benefit of lower image file sizes, thus lower bit-rate and bandwidth usage. At the same time the frame rate can be easily controlled, providing a means to limit bandwidth usage by reducing the frame rate, but still with a guaranteed image quality.

Since MJPEG does not make use of a video compression technique, it generates a relatively large amount of image data that is sent across the network. For this reason, at a given image compression level (defining the image quality of the I-frame and JPEG image respectively), the network bandwidth is less for MPEG compared to MJPEG, except at very low frame rates.

Another difference is that most MJPEG IP cameras can produce multiple simultaneous streams and in different qualities (image sizes and compression quality) while most MPEG cameras can produce only one stream in one quality. Therefore the same stream will be used in live viewing and recording.

This summarizes the benefit of MPEG: the ability to give a relatively high image quality at a lower bit-rate (bandwidth usage). This can be especially important if the available network bandwidth is limited, or if video is to be stored (recorded) at a high frame rate and there are storage space restraints. The lower bandwidth demands come at the cost of higher complexity in encoding and decoding, which in turn contributes to a higher latency when compared to MJPEG.

The graph below shows in principle how bandwidth use between MJPEG and MPEG compares at a given image scene with motion. As can be seen, at very low frame rates, where MPEG compression cannot make use of similarities between neighboring frames to a high degree, and due to the overhead generated by the MPEG streaming format, the bandwidth consumption is actually higher than MJPEG.



1.4.5 JPEG image sizes and storage requirements

The image (recording) quality and image size affects the required storage per image (frame). Likewise does the frame rate impact the recording storage and also the network bandwidth.

VisoGuard supports all image sizes that a camera offers. The following are some **values for typical JPEG images**:

JPEG Image size	Image quality	Storage per image approximately
Small 176x144 QCIF PAL 176x120 QCIF NTSC 160x120 QQVGA	Low	3 KB
	Medium	5 KB
	High	8 KB
Medium	Low	8 KB

JPEG Image size	Image quality	Storage per image approximately
352x288 CIF PAL 352x240 CIF NTSC 320x240 QVGA	Medium	13 KB
	High	20 KB
Large* 704x576 4CIF PAL 704x480 4CIF NTSC 640x480 VGA	Low	20 KB
	Medium	34 KB
	High	52 KB

* For mega-pixel cameras the image size will be much bigger than shown in the table.

2 Starting and operating the VisoGuard client

2.1 Introduction the VisoGuard client

Once you have successfully installed VisoGuard on your server, authorized users can access the server via an VisoGuard client.

Normally the VisoGuard client runs on a PC separate from the server, however in a client-on-server installation the client runs directly on the server (see the document *Thecus VisoGuard 4.0 Server Installation and Administration* for further information on how to create and run a client-on-server installation).

Licensing issues

The available functionality of your VisoGuard installation is defined by the license string. The document *Thecus VisoGuard 4.0 Server Installation and Administration* describes how licensing works and how to obtain a license string. If you have a temporary demo license, a **License** dialog appears at every login indicating that there is no permanent license. At this dialog just push the **Continue** button to operate VisoGuard in the demo mode.

See *10.1 Server system information and restarting* on page 72 for how to display the current license of your server.

Different clients

You can choose among these VisoGuard clients, operating systems and platforms:

VisoGuard client	OS and platform	Supported functionality
Locally installed client	MS Windows 7, XP, Vista, etc.	All
	Linux, Unix (also client on server)	No audio, layout navigation, and PTZ-Joysticks; Mac OS-X: additionally no MPEG streaming (MPEG-4, H.264, and MxPEG)
Standard web browser	MS Windows 7, XP, Vista, etc.	No layout navigation and Joysticks for PTZ control
	Linux, Unix	No audio, layout navigation, and PTZ-Joysticks; Mac OS-X: additionally no MPEG streaming (MPEG-4, H.264, and MxPEG)
Mobile client	Apple iPhone and iPad	Online viewing only

Please be aware that some functions like Layout Navigation and running SAFE export files may only be available on the MS Windows platform.

This chapter describes how to start the VisoGuard client on a desktop PC. If you want to run VisoGuard on a mobile device please refer to *12 VisoGuard on mobile devices* on page 83.

The minimum screen resolution for running the VisoGuard client is 1024x768 pixels.

2.1.1 Advanced client technology

The VisoGuard uses advanced technologies to ease the operation of clients on MS Windows platforms:

- **Lazy-loading client technology**: VisoGuard clients (both browser-based and locally installed) only load the needed application components from the server on demand, when they are needed. This saves time at startup and also bandwidth. It also eases the management and upgrading of clients. Libraries for one version are downloaded only once and are now stored locally on the client machine. The path is <user's home directory>\netavisLibs\<version> (e.g. D:\Documents and Settings\user\ netavisLibs\1.9.0.110.200).
- **Automatic client upgrading**: Whenever the VisoGuard server is upgraded to a new version, the clients are automatically upgraded too. This is happening transparently to the user. The same client will still be able to work with older server versions (see next point). Starting with release 1.9 the client application has to be installed only once and every further VisoGuard version will be seamlessly accessible, without having to manually upgrade the client.
- **Different versions between servers and clients**: Starting with release 1.9 VisoGuard clients can connect to servers running different versions (release 1.9 or newer) without the need to install clients matching the servers' versions.

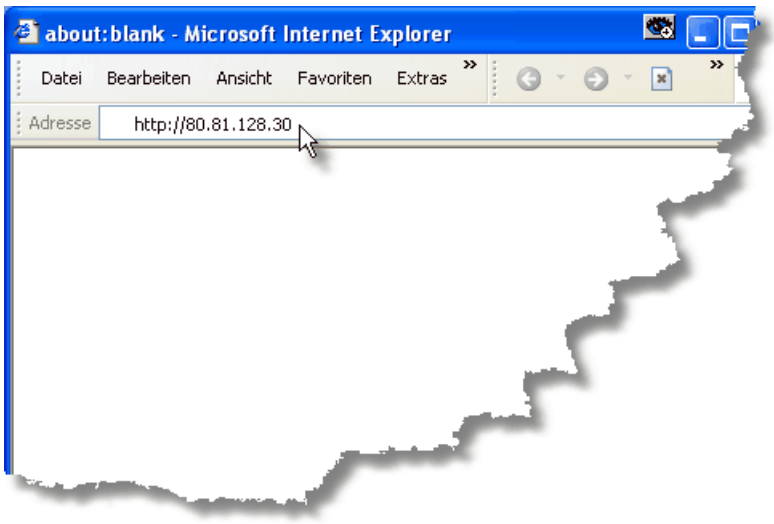
As a summary, VisoGuard clients...

- …download libraries (for one version) only once
- …share the same libraries for both browser-based (applet) and installed client application
- …can connect to servers having different versions
- …automatically upgrade themselves when the server has a new version

2.2 Starting the VisoGuard client in a standard web browser

This section describes how to start the client in a standard web browser. If you want to install the client on your machine and run it independently of a web browser, please refer to *2.3 Working with the installed VisoGuard client* on page 14.

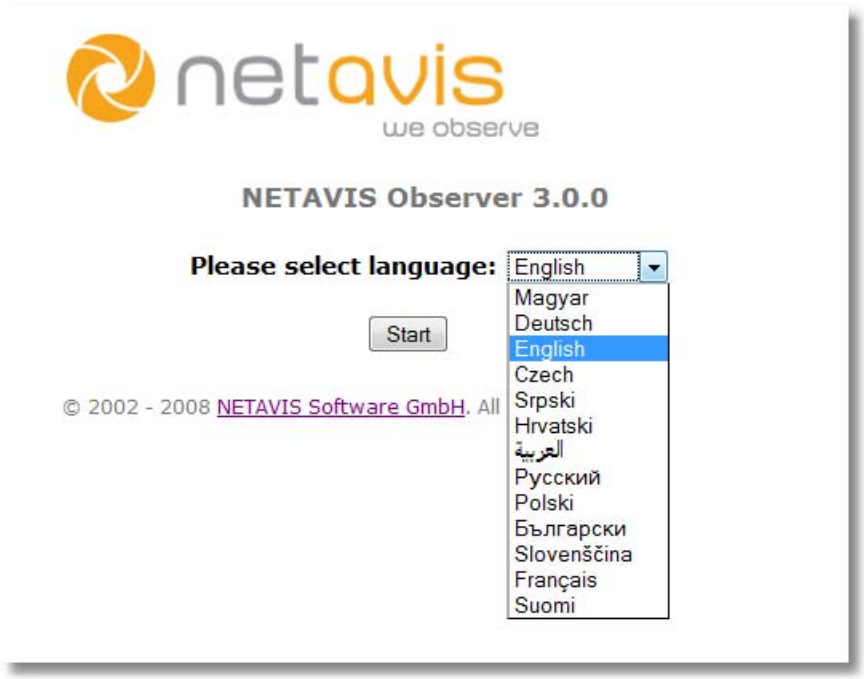
1. Launch an Internet browser and enter the address of your server: http://IP-address-of-your-server:8080



Now a page that checks the availability of the Java on your computer appears. This page should disappear in a few seconds.
If this page stays, it means that you do not have the Java plug-in installed on your browser. You have to first install Java by visiting www.java.com/download to install the latest Java 2 package

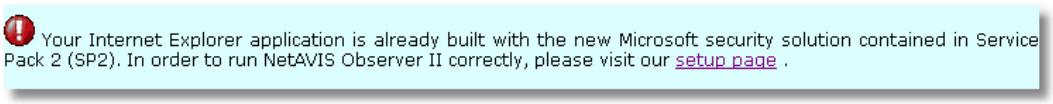
and then start the browser anew. Now the screen should disappear and you can continue as shown below.

Next a startup screen is displayed that lets you choose the language that you want VisoGuard to use.



2. Click on your language of choice and push **Start**. This takes you to the start page of VisoGuard:

   If your browser is Internet Explorer and client system is Windows XP SP2 (service pack 2) then a special paragraph is shown explaining that additional browser settings are necessary:


Your Internet Explorer application is already built with the new Microsoft security solution contained in Service Pack 2 (SP2). In order to run NetAVIS Observer II correctly, please visit our setup page .

   Follow the link and apply the settings as described on the SP2 page. After that restart the browser and continue.

3. After you click on **Start Thecus VisoGuard**, you will be advised that the program is being loaded. How long loading takes depends on your network.
   On completion of loading, you will be notified that VisoGuard is initializing. Then user data is loaded.

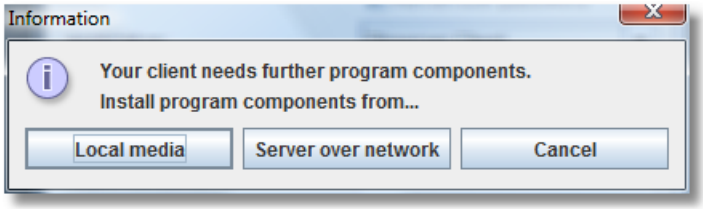
Note: By clicking on **Download Thecus VisoGuard client installer** you can also install the VisoGuard client on your machine locally. *2.3 Working with the installed VisoGuard client* on page 14.

4. Before starting the VisoGuard client you will be asked if you allow to execute the downloaded trusted applet:

Sicherheitswarnung
Installieren und Ausführen von "NetAVIS Observer II", signiert zu einem unbekannten Datum/Uhrzeit und herausgegeben von:
Xperts Software Ltd.
Authentizität des Herausgebers bestätigt durch VeriSign Class 3 Code Signing 2001 CA
Hinweis: Xperts Software Ltd. versichert, dass dieser Inhalt sicher ist. Die Installation bzw. das Anzeigen des Inhalts sollte nur erfolgen, wenn Sie Xperts Software Ltd. vertrauen.
Zugelassene Signatur
Volle Zugriffsrechte
Inhalt von Xperts Software Ltd. immer vertrauen
Ja
Nein
Weitere Informationen

Select the checkbox **…always trust…** and click on **Yes** to allow the download of the trusted applet.

When you start the client the first time after a new installation some additional client application components need to be installed (this is needed only once per client). You will be asked:



Normally you want choose to install the program components from **Server over network**. However, if you have a very slow network connection between the client and the server you might want to choose installation from **Local media**. When you choose this option you will be asked to locate the directory **ClientInstaller** of the VisoGuard installation CD. Once you choose the correct location and push OK, the components will be installed.

5. Next you either come to the login panel or to the license dialog.
If the license dialog appears you yet have to obtain a license for using VisoGuard. Please consult the manual *Thecus VisoGuard 4.0 Server Installation and Administration* for information on how to do that.
At the login panel enter your **Login name** and **Password** and click **OK**.

If you do not yet have a permanent license string for VisoGuard, a **License** dialog appears. To continue without a permanent license just push **Continue**. In this case the full functionality may not be available. See also *2.1 Introduction the VisoGuard client* on page 10 for further details about licensing.

Please note: The authentication data transferred between client and server are encrypted with MD5 strong encryption (only if you use Java VM 1.4 or newer, otherwise unencrypted).
The administration user **admin** has the default password **admin**. For security reasons you should change this password (please see *4 Managing users* on page 29).

A guest login is possible only if the guest has been defined on your server (which is the factory setting). For further details contact your VisoGuard administrator.

If you have forgotten your password, you can mark the **Forgot my password** checkbox, answer the asked question, and click **OK**. For more information, ask your VisoGuard administrator.

2.2.1 What is next

If your VisoGuard server already has cameras configured, then you can go to chapter *5 Using the Online monitor* on page 34. If you have to setup cameras first, then continue with chapter *3 Setting up cameras* on page 20.

Furthermore, because VisoGuard behaves in a context-sensitive way, you will find that certain menu items are also disabled at certain times. Thus, for example, you cannot remove a camera if there is no camera to remove. Thus in different contexts the same menu might look quite different at different times (menu entries and buttons in grey are disabled and in black are enabled).

2.3 Working with the installed VisoGuard client

Alternatively to starting the VisoGuard client from a web browser you can also install the Java client application locally on your machine. Some functions are only available in the installed client (see *2.1 Introduction the VisoGuard client* on page 10 for details).

2.3.1 Installing the VisoGuard client

To **install** the client locally, please follow these steps:

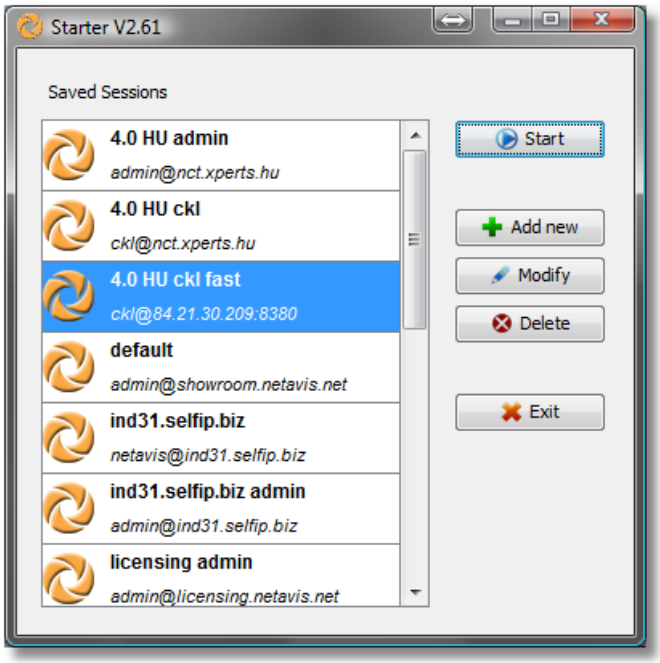
1. At the **VisoGuard Start page** click on the link **Install the VisoGuard client on your PC (using Web Start)**.
2. Save and run the Web Start installer.
3. Follow the steps of the setup program.

Alternatively you can also download and run the client installer executable on Windows platforms:

1. At the **VisoGuard Start page** click on the link **Alternative installation: Download VisoGuard client installer executable (Windows only)**.
2. Save the client installer executable at an arbitrary location.
3. Execute the just downloaded client installer (Observer_setup.exe).
4. Follow the steps of the setup program (standard Windows installation).

2.3.2 Starting the installed VisoGuard client

Once the setup finished you can start the client locally from your Windows **Start** menu (or also from a desktop icon if you selected so at installation). The **Starter** window appears:



Working with sessions

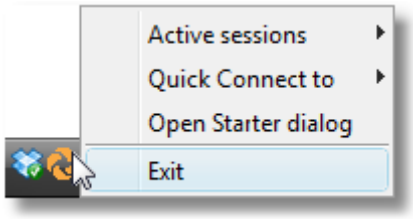
The **Starter** allows you to manage sessions. In a session you can define the server address, which VisoGuard application to start and the user/password details. Thus you can store and run different sessions easily.

The **Session editor** is opened when you push **Add new** or **Modify** and allows you can define the session details:

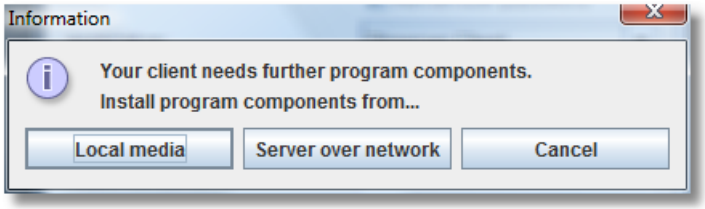
Element	Meaning
Session name	Name under which the session is stored.
Application	You can either choose **VisoGuard Client** or **Layout Navigation Tool** (for further details on the Layout Navigation Tool please refer to *13 Working with Layout Navigation* on page 84). The selected application will start when you press **OK**.
Previous Sessions	Offers you the list of previously active sessions.
Hostname or IP Address	Enter the name or IP address of the server you want to connect to.
Username	Enter the login name of the user.
Password	Enter the password for the user.
Remember password	Select the checkbox if you want the password to be remembered for the next start of the application.

Starting the client

Pushing **Start** in the **Starter** will open the client window and connect you to the VisoGuard server. When the client is started, the **Starter** window will be hidden and in the task bar you will see it's icon. You can access the Starter by clicking its icon. There you can open the Starter dialog again and also force an exit of the client application.



When you start the client the first time after a new installation some additional client application components need to be installed (this is needed only once per client). You will be asked:



Normally you want choose to install the program components from **Server over network**. However, if you have a very slow network connection between the client and the server you might want to choose installation from **Local media**. When you choose this option you will be asked to locate the directory **ClientInstaller** of the VisoGuard installation CD. Once you choose the correct location and push OK, the components will be installed.

If you do not yet have a permanent license string for VisoGuard, a **License** dialog appears. To continue without a permanent license just push **Continue**. In this case the full functionality may not be available. See also *2.1 Introduction the VisoGuard client* on page 10 for further details about licensing.

Working with sessions of pre-4.0 servers

The **Starter** also allows you to also manage sessions with VisoGuard servers running a releases older than 4.0. Just select the checkbox **Show settings for pre-4.0 releases** to show the additional settings.

Description of elements:

Element	Meaning
Window width, height	Define the size of the client window in pixels.
Upper left corner X, Y	Define the location of the upper left corner of the client window in pixels. This setting can be changed, e.g., for multi-screen setups.
Initial monitor view name	Is optional and defines the initial **Online monitor** view.
Window decoration visible	Defines whether the windows decoration border is visible.
Tool control bar visible	Defines whether the tool control bar at the right side of the window is visible. This bar allows switching between Online Monitor, Archive Player, Event Management and Administration.
Event bar visible	Defines whether the event bar at the bottom of the window is visible.
Online monitor control bar	Defines whether the menu and the history buttons for Online

Element	Meaning
visible	monitor control are visible.
Overlay painting enabled	When this is selected and the hardware supports it the Online monitor uses the hardware overlay technique for displaying flicker-free MPEG streams. This can also boost the client performance and relieve the main CPU. In multi-screen operation, overlay painting of MPEG video streams may result in pink colored view ports if the client is not running on the primary screen of Windows. Then you should turn off this feature.

2.4 Client multi-window and multi-screen operation

VisoGuard supports multi-window and multi-screen operation. With clients that have multiple screens connected you can position windows at different screens.

Here is an example of a client setup with 3 screens:

The window contents and positions are automatically stored per user and between sessions. This means when a user has multiple windows positioned on 3 screens and he exits and then logs in again, all the windows on the 3 screens will automatically be restored.

Please note: There can only be one Archive player and this is located in the main window.

2.4.1 Creating a new window

In the main application window select **New window** from the **Windows** menu.

The window title and the contents of the window can be adapted by choosing **Client preferences...** in the VisoGuard menu (see below).

2.4.2 Defining what components to display in a window

For each window you can define which of these components should be displayed in the window:

- Online Monitor
- Archive player

- Event list
- Camera tree

You can define any combination of components and you can also define that a window should contain only one component.

Note: Depending on the authorization that your VisoGuard administrator has assigned to you, some of the client components could be disabled (menu shown in grey color). If you need more authorization, please contact your local VisoGuard administrator.

Here is how you can define what components are to be shown in a window:

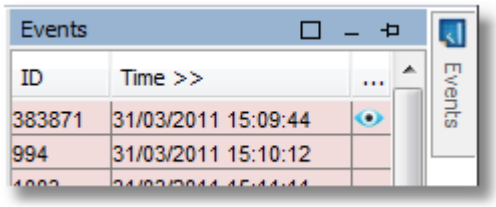
1. In the VisoGuard menu choose **Client preferences...** which will open the dialog.
2. For each window you can define what should be displayed. For example, select the **Online monitor** node and turn on (select) the **Display Online monitor** check box. For each window individually you can turn on or off the **Event list**, **Camera tree**, and **Archive player** (only for the main window).

   Please note: Normally it does not make sense to always show the camera tree since it will be opened when needed on demand.

2.4.3 Modifying window layouts

You can also modify the layout of a window by rearranging its components. Once you have defined in the **Client preferences** dialog what components are to be shown in a window you can customize the layout. Select the menu **Windows**->**Enable layout customization**. For the Event list and the Camera tree you can now define:

- Where they are located inside the window: Just click on the title bar of the Event list or the Camera tree and drag it to a different location. For example, when the Online monitor and the Event list are enabled, then you can drag the Event list from the default position at the right border of the window to the bottom of the window.



- Whether they are floating (open when needed or there are new entries and collapsed or hidden otherwise) or pinned (always shown): You can change the state of the Event list or the Camera tree by pinning or unpinning it in the title bar.

  Whether the Event list or the Camera tree should fill the whole window: You can maximize the component by pushing the maximize button. When a component is maximized, it will occupy the whole space of the window and will automatically resize when you resize the window. Thus you can create a window that contains only an Event list.

After you are done with the modifications deselect **Windows**->**Enable layout customization**.

The default location for the Event list is the right window border and for the Camera tree (that usually only pops up when needed) it is the left window border.

Please note that only the Event list and the Camera tree can be dragged. The other components in the window will then change their size accordingly.

2.4.4 Deleting a window

In the main application window select **Delete window...** from the **Windows** menu. A **Delete window** dialog will open, offering you the list of available windows for deletion.

2.4.5 Positioning a window on a certain screen

Positioning a window on a certain screen is very easy: With the mouse just drag the window to the screen and drop it there. You can also maximize the window on the screen. All the window states will be remembered between sessions. This happens on a per-user basis, which means when the user is logging in on a different client workstation he will have the same window setup as on the first client workstation.

2.5 VisoGuard Transcoding™ for low-bandwidth client-server connections

The unique VisoGuard Transcoding™ technology reduces the necessary bandwidth for video streams to a fraction of the usual values. Especially high-resolution cameras can thus be streamed from server to clients over low-bandwidth wide areas network (WAN) connections without loss of quality. Therefore even megapixel cameras can be operated over very low bandwidth connections that would normally prevent their operation. The technology works for all cameras, streaming resolutions, and formats (including MPEG-4, H.264, and MxPEG).

Additional CPU resources are needed at the server and at the client for transcoding streams.

Transcoding™ can be set up by limiting bandwidth for live video and recording playback streams at the server level (defined in *10.2 Setting VisoGuard server parameters* on page 75).

Important: Although transcoding works with all streaming formats, the **best results and least CPU overhead** are possible with MJPEG streaming. Also the transcoding bandwidth limit must be chosen carefully.
Therefore **we suggest:**
• MJPEG streaming format.
• Limit the transcoding bandwidth to app. 70% of the available server-client connection bandwidth.
For connections, like Internet connections, with heavily varying bandwidth it is much better to use a lower limit than a higher limit. With low limits of 256 kbit/s or 128 kbit/s very good results are possible. Some customers have even used 56 kbit/s or 30 kbit/s with transcoding.
As indicated above the limits are defined in *10.2 Setting VisoGuard server parameters* on page 75.

2.6 Exiting the client

The VisoGuard client can be exited by choosing **Exit** from the **VisoGuard** menu at the main application window. You will be asked whether you really want to exit.

If the menu bar is hidden, you can exit the client via the right mouse button menu.

3 Setting up cameras

VisoGuard allows any authorized user to set up cameras in the system. Ask your VisoGuard system administrator whether you have such authorization.

3.1 Preparations

Before you begin to set up a new camera in VisoGuard, be sure to have the following information available:

- Your camera type.
- Is your camera type supported by VisoGuard?
  Please consult the document *Thecus VisoGuard 4.0 Supported Video Sources*.
- Are there available licenses for setting up additional cameras?
- IP addresses of cameras (or camera servers).

Please note: Here we describe how to setup a camera in VisoGuard. If you setup an IP camera, then the camera itself also can be configured. This is normally done via a web-based interface of the camera. Please consult the manual of your IP camera for further details.

3.2 Adding a new camera and setting basic properties

Start the VisoGuard client application (see *2 Starting and operating the VisoGuard client* on page 10).

You can either

- add a new camera from scratch, or
- duplicate an existing camera and just modify some parameters (see *3.2.2 Duplicating an existing camera* on page 26). Duplicating an existing camera creates an exact duplicate with all settings copied. This is useful when you have more than one camera of the same type or with equal/similar settings (like recording or video analytics settings).

3.2.1 Adding a camera from scratch

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. With a mouse click, select the camera group to which you want to add the new camera (later on you can move the camera in the camera tree to a different group).
3. Choose **Add new camera** from the menu.

   The **Properties** dialog opens in which you can configure the camera.
   Enter your camera data in the corresponding fields. Use the following table as a guide. Fields labeled in **bold** are **mandatory** while all others are optional:

Field label	Your input
Camera name	Enter the name that you want to give your camera. This is the name by which you will select or display this camera (e.g., camera 2).
Comment	Here you can add text that describes your camera.

Field label	Your input
Time zone	Select the time zone of your camera's location (e.g., CET for a camera installed in Vienna).
Camera type	Specify the type of camera by selecting it from the camera pop-up menu. **Important**: If you want to connect an analog camera via a video server then select the type of the video server from the menu. If you connect an analog camera to a video capture card directly in the VisoGuard server, then select **NDS** (VisoGuard Digitizer Server) as your camera type.
Name of camera admin	If the camera needs authentication for administrating, then enter the user name of the camera administrator here.
Pwd of camera admin	Enter the password of the administrator account of the camera (only if used).
Camera IP address	Specify the IP address or network name of your camera or video server. If you supply a network name, you must have access to a domain name server (DNS) that resolves the name to an IP address. Even dynamic DNS names (like dyndns) can be used. This field is not needed for analog cameras connected directly via a video capture card (NDS).
Camera server port	If you are adding an analog camera via a video capture card (NDS) or via a video server, specify the port of the capture card or video server to which the camera is connected.
Aspect ratio	This setting is only enabled for certain IP cameras that are shipped with different aspect ratios (like PAL or NTSC). For cameras that are delivered in one standard only, the correct value is set automatically and cannot be changed. Please select the correct value for your camera. If you select a value that does not fit your camera, then the image might be distorted. Please refer also to *1.4.5 JPEG image sizes and storage requirements* on page 8.
Streaming mode (Mobotix only)	This option is only relevant if you use a Mobotix camera. Set it when you would like to operate the camera in streaming mode. If this option is not activated, the camera operates in single picture mode. In streaming mode (MJPEG format) the camera delivers higher frame rates than in single picture mode. If you activate the streaming mode you also must set the according option in the camera with the Admin tools of the camera.
Use HTTPS encryption	If the camera supports encrypted streaming using HTTPS this setting will be enabled. It defines whether streaming from the camera is encrypted using HTTPS. Please note that encryption needs significantly more CPU resources on the server than unencrypted communication (see also *1.3 VisoGuard data security* on page 5).
Non-interlaced mode	This option is only relevant for digital cameras or video servers that

Field label	Your input
enabled	support 2CIF resolution to reduce the interlace effect. Please refer to the camera's documentation.

Push **Save** to create the new camera.

4. Select the newly created camera again in the camera tree and then push the **Next** button at the bottom. This invokes the **Default settings** dialog that lets you define the default image and audio settings for your camera. To modify values choose **Modify selected camera or group** menu.

   Fields for **Basic video and audio settings**:

Field label	Your input
Multi stream allowed	Some cameras are capable of providing multiple video streams in parallel. This can be helpful for example, when online viewing and recording is to be done in different formats or for optimizing iCAT video analytics performance (see *1.4 Video streaming methods and compression* on page 6 for a general discussion about multi streaming). Usually MJPEG cameras can deliver several MJPEG streams while MPEG (MPEG-4, H.264, and MxPEG) cameras deliver only 1 MPEG stream (some camera types can deliver several MJPEG streams in addition to the MPEG stream). If this option is not selected, then only 1 video stream will be pulled from the camera regardless of how many different formats would be needed. If it is selected then multiple streams will be pulled. Also consider the following checkboxes that define, which formats can be pulled from the camera. **Please note:** Multi-streaming has some important restrictions that depend heavily on the camera type. Please refer to the document *Thecus VisoGuard 4.0 Supported Video Sources* for details on restrictions.
Allow JPEG streaming	If your camera supports MJPEG video streaming, you can allow using this mode by selecting this checkbox. In one special case, VisoGuard will try to pull an MJPEG stream even if this checkbox is deselected. This is the case when iCAT video analytics is working on MPEG streams (e.g. for motion detection) and **Multi stream allowed** is selected. This special additional MJPEG stream in QVGA is used only for iCAT and helps to minimize server CPU load for iCAT processing (please refer also to *14.2.1 Considerations for setting up a system with iCAT* on page 97).
Allow MPEG-4 streaming	If your camera supports MPEG-4 video streaming, you can allow using this mode in the Online Monitor and the archive by marking this checkbox. Please note that platform restrictions may apply for this streaming mode (please refer to *2.1 Introduction the VisoGuard client* on page 10).

Field label	Your input
Allow H.264 streaming	If your camera supports H.264 video streaming, you can allow using this mode in the Online Monitor and the archive by marking this checkbox. Please note that platform restrictions may apply for this streaming mode (please refer to *2.1 Introduction the VisoGuard client* on page 10).
Allow MxPEG streaming	If your camera supports MxPEG video streaming, you can allow using this mode in the Online Monitor and the archive by marking this checkbox. Please not that platform restrictions may apply for this streaming mode (please refer to *2.1 Introduction the VisoGuard client* on page 10).
Stream MPEG-4 via Multicast	This option should only be switched on in very special situations. When marked then the MPEG-4 stream from the camera is received via "multicast", when disabled via "RTSP over HTTP". Multicast is a one-to-many, while RTSP is one-to-one type connection. Mark this checkbox only if you want to have multicast MPEG-4 streaming of the camera. In most cases you want to leave this checkbox not marked, which means that the MPEG-4 stream is transmitted via RTSP over HTTP.
Allow Audio to camera	When marked, VisoGuard will allow Audio to the camera and will offer a button for that in the **Online Monitor**. Of course this feature only works if you have a working microphone connected to the PC where you run your client on and your camera has a loudspeaker function.
Allow Audio from camera	When marked, VisoGuard will allow Audio from the camera to your client (in the **Online Monitor** and for recordings). Of course this feature only works if you have a working loudspeaker connected to the PC where you run your client on. Please note that platform restrictions may apply for this streaming mode (please refer to *2.1 Introduction the VisoGuard client* on page 10).
Audio from and to share single button	If this checkbox is marked, then there is only one button in the **Online Monitor** that switches MPEG and Audio on and off. If this checkbox is not marked, then you will find 3 buttons for the three functions. See also *5.9 Working with MPEG cameras and audio ()* on page 41.
Anonymize (distort) audio	In some cases Laws do not allow the transmission or recording of people's voices. The criterion often is whether one can recognize a person by listening to its voice. Therefore VisoGuard allows anonymizing the audio stream by distorting it. If this checkbox is marked then the live and recorded audio will be anonymized (distorted).

The **Default settings for MPEG-4, H.264, MxPEG** and **Default settings for single-stream JPEG cameras** define the streaming format for the various streaming types. These settings will

be used in the **Online Monitor** and also for recordings. For multi-stream JPEG cameras, the **Default settings for single-stream JPEG cameras** are of no importance (because for each view port in the Online Monitor and also for recording separate formats can be specified).

Please note: In the current version, VisoGuard only supports 1 streaming format for MPEG cameras for live viewing and recording.

Field label	Your input
Use these settings	Usually this checkbox must be set. It defines whether the default camera settings are set via VisoGuard or in the camera directly (via its own setting utilities). When it is switched on, the settings in the camera are overwritten by the values of this dialog. When it is switched off, the values from the camera are taken and the settings in VisoGuard are ignored. In very special situations only, e.g. when setting the values by VisoGuard causes some unwanted side effects in the camera, you may want to set the values in the camera directly and switch off this check box.
Image quality	Defines the image quality of the stream. The possible values are **High**, **Medium**, and **Low** quality. The higher the quality, the more bandwidth will be used for transmission and the bigger the space requirements for recording will be (see also *1.4 Video streaming methods and compression* on page 6). For multi-stream JPEG cameras, this value cannot be set here, since separate image qualities can be set for recording and in each view port in the Online Monitor.
Image size	Defines the image size of the stream. Possible values depend on the camera model. The bigger the image size, the more bandwidth will be used for transmission and the more space for recording will be needed. For multi-stream JPEG cameras, this value is of no importance, since separate image sizes can be set for recording and in each view port in the Online Monitor.
Frame rate	Defines the frame rate of the stream. Possible values depend on the camera model. The bigger the frame rate, the more bandwidth will be used for transmission and the more space for recording will be needed. For single-stream JPEG cameras, this value defines the maximum possible frame rate. In the Online monitor and for recording lower frame rates can be selected.
GOP size	For MPEG streams defines the how many frames are sent and stored in a GOP (group of pictures). One GOP is an integral data packet that is transmitted and recorded. Our default value is 10, which means that there is 1 reference frame (I frame) and 9 difference frames (P frames). A bigger GOP size means a higher compression rate but also a somewhat lower quality and a bigger delay between a real scene and its viewed images (which is relevant, e.g. for live viewing in the Online Monitor). We think that a GOP size of 10 is optimal for most case, which, dependent on camera model, covers a time between 0.5 ~ 1 sec.

Field label	Your input
Bandwidth limit (Kbps)	This setting limits the maximum bandwidth in kilobits per second for the transmission of MPEG streams between the camera and the server. As a consequence, also the bandwidth between the server and the clients is thus limited and also the required storage in the archive is influenced (limited). If this value is zero, then the bandwidth is not limited. This actually is a setting in the camera. The camera always optimizes for the desired image quality and will sacrifice frame rate in favor of quality in the case, the bandwidth would exceed the supplied limit.

Fields for **In-camera motion detection** (please refer to *7.3 In-camera motion detection* on page 59 for further details):

Field label	Your input
Receive event images via FTP	If this checkbox is marked, you enable the In-camera motion detection and tell VisoGuard to receive event images via FTP. Please be aware that if you select this checkbox, the server-based motion detection must be disabled.
Receive event images via HTTP	The same as above, just that the images are received via HTTP protocol (some cameras support only HTTP).
Post recording length (sec)	When VisoGuard receives an in-camera event, then it can start a parallel server-side recording in addition to the event images it receives from the camera. The event images received from the camera via FTP/HTTP are merged with this server-side recording. This field defines how long this parallel post-event recording is. If it set to 0, then VisoGuard does not start its own server-side recording of images and just stores the event images it receives from the camera via FTP/HTTP.
Recording frequency	This field defines the recording frequency of the above mentioned parallel server-side post-event recording.

5. Push the **Next** button at the bottom of the dialog. This invokes the **Scheduling** dialog. Please refer to *6.1 Programming archive recordings* on page 43 on how to set up the camera archive and scheduling.
6. Optional: Push the **Next** button again at the bottom of the dialog. This invokes the **I/O Control** dialog that lets you define the handling of optional I/O contacts of your camera. If you do not want to use I/O contacts you can just jump to the next step.

   Set your values:

Field label	Your input
Input handling enabled	Select this check box if you want to process the state of the digital input-contact port of the camera.

Field label	Your input
Input poll interval (msec)	The poll interval defines how often the state of the input port is checked. Minimum time is 500 milliseconds.
Output handling enabled	Select this check box if you want to enable switching the digital output port of the camera from within view port menu.

7. Push the **Save** button at the bottom of the dialog.

3.2.2 Duplicating an existing camera

Duplicating an existing camera creates an exact duplicate of the camera with all settings copied. This is useful when you have more than one camera of the same type or with equal/similar settings (like recording or video analytics settings).

With duplicating camera you can dramatically reduce the set up time for systems with many cameras with similar settings.

Here is how you can do that:

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. In the camera tree select the camera you would like to clone.
3. Choose **Duplicate camera** from the menu.

   Now a new camera named as the existing camera with "(copy)" appended has been created.
4. Set the basic properties like name and IP address.
5. Optionally modify other parameters as needed (see *3.2.1 Adding a camera from scratch* on page 20 for details).
6. Push the **Save** button at the bottom of the dialog.

3.3 Setting up the camera recording archive

The configuration of camera recordings is covered in section *6.1 Programming archive recordings* on page 43.

3.4 Optional: Configuring video analytics (iCAT)

The configuration of video analytics with iCAT is covered in chapter *14 Video analytics with iCAT* on page 96.

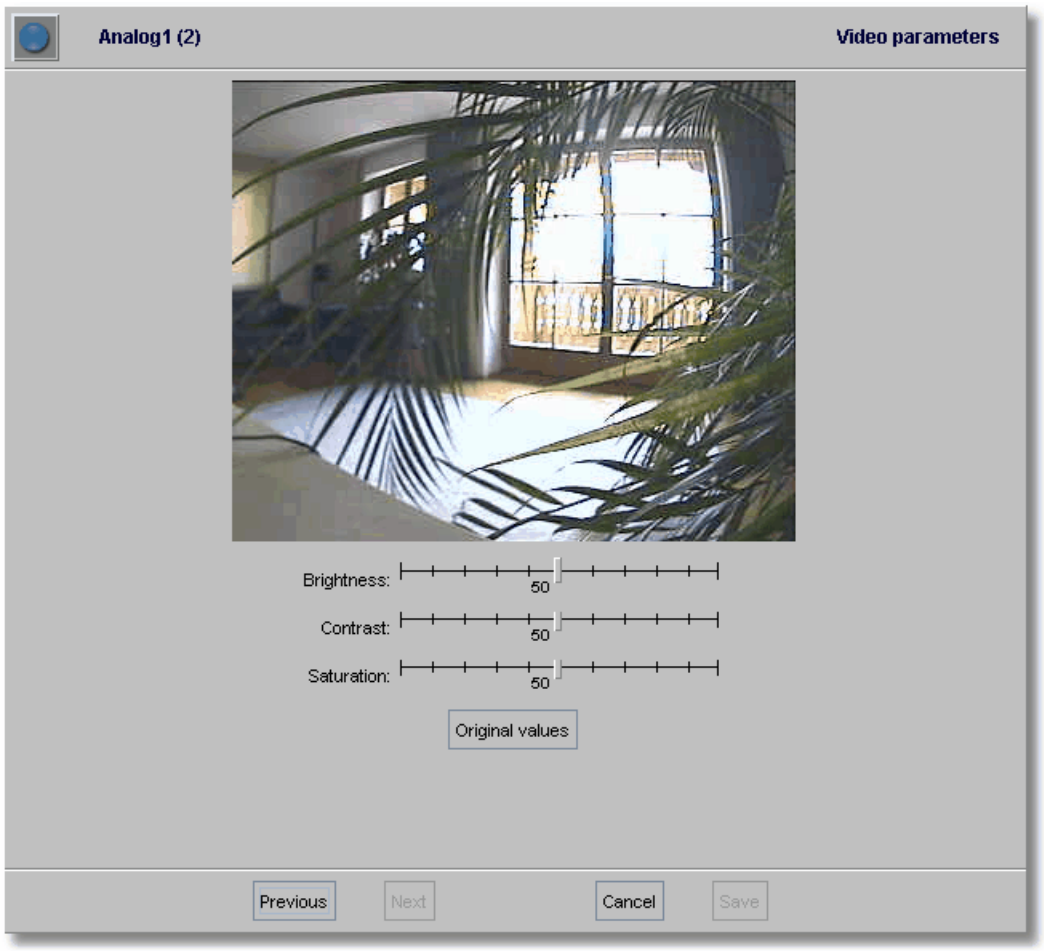
3.5 Defining brightness, contrast, and saturation

If you are not satisfied with the brightness, contrast or saturation of camera video images then you can modify them. For IP cameras and analog cameras there are two different ways of modifying those video parameters:

- **IP cameras**: Each IP camera has its own setup interface (usually available via web browser) to define / modify the video parameters. Please consult the admin / setup manual of the IP camera.
- **Analog cameras**: VisoGuard allows you to define video parameters via the System Admin menu. Please see below for details.

3.5.1 Defining video parameters for analog cameras

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. Select the camera in the camera tree for which you want to set the image values.
3. Press the **Next** button 4 times (starting from basic properties to scheduling to I/O control to Image settings. Now you should see the **Video parameters** dialog:



4. In the menu select **Modify selected camera or group** and then modify the brightness, Contrast and Saturation values according to your needs. Please be aware that light conditions may change during the day.
5. To store the settings press **Save**.

3.6 Working with camera groups

Camera groups are a powerful means for managing and organizing cameras.

3.6.1 Creating a new camera group

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. In the camera tree select the group in which you want to create the new camera group.
3. In the menu select **Add new camera group** which will open new dialog that allows you to enter the name and description for the new camera group.

4. Optionally select the **Use group name as camera name qualifier** checkbox. If this checkbox is selected then the name of the camera group is displayed as prefix to the camera name, e.g. “group-name:camera-name”.
5. Press **Save** to create the new camera group.

3.6.2 Moving a camera or camera group in the camera tree

A camera or a group of cameras in the camera tree can be moved to another location by following these steps:

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. With a mouse click choose the camera or group you want to move.
3. In the menu select **Move camera or group**.
   A new dialog appears that requires you to enter the password.
4. Enter the password.
   After you enter the correct password a camera group dialog is opened showing the camera groups.
5. In the newly opened camera groups dialog select the group where you want to move the camera or group to and press **Select**.
   Now the camera or group is moved to the new location and the camera tree is updated.

3.7 Changing the port mapping of analog cameras

This section is only valid for analog cameras. For analog cameras a port must be defined where the camera is connected to at the video capture card or the video server.

Sometimes the port mapping of analog cameras needs to be changed but it is difficult to do that physically by changing the cabling. To help the situation, VisoGuard can change the port mapping in the software.

There are two ways for doing that:

- Either go to the **Camera Administration** and manually switch the port there. For this however you need to know exactly which camera is connected to which port.
- You can also swap the ports in the **Online Monitor**. This has the advantage that you see the video pictures and therefore you can identify the correct ports visually.

In order to swap the ports of two analog cameras visually please follow these steps:

1. In the **Online Monitor** go to the view that shows the first analog camera in a view port.
2. CTRL-click into the view port that shows the first analog camera.
3. Now go to the view that shows the camera that you would like to swap with and CTRL-click in the view port.

Now the ports of the two cameras have been swapped.

4 Managing users

VisoGuard requires users to login in order to work with the system. This chapter describes how to create and manage users in VisoGuard.

Generally, you can either

- use VisoGuard to administer users (see *4.1 Creating a new user account* on page 29), or
- utilize Active directory or LDAP to manage users (see *4.8 Working with users from Active Directory or LDAP* on page 32).

4.1 Creating a new user account

An VisoGuard administrator can create user accounts in the system.

Please note: At initial product installation of a set of predefined users accounts and groups are created. These users and groups model typical permissions of users in various roles. Instead of creating a new user account you can take one of these predefined users and modify the settings accordingly.

Here are the steps for creating a new user account:

1. Choose **User admin** from the **System administration** menu. This opens the **User admin** dialog.
2. Select a user group to which you want to add the user. Please refer to *4.4 Working with user groups* on page 31 if you want to create a new user group first.
3. In the menu select **Add new user**. The **Properties** dialog opens to allow you to enter user data.
4. Enter your user data in the corresponding fields of the dialog. Use the following table as a guide. Fields labeled in **bold** (both in the dialog and in the table) are **mandatory**; all others are optional:

Field label	Your input
Login name	This is a short name that the user will use to log in.
Full user name	This is the complete name of the user.
Password	Enter a password for the user. The user can change this later on (see *4.7 Changing the password* on page 32).
Re-enter password	Enter the password again for verification.
Secondary password	Enable the checkbox and enter a secondary password if a secondary password is needed for logging in the user. This is important for enforcing the four-eyes principle for certain video operations.
Re-enter sec. password	Enter the secondary password again for verification.
Forgot question	Formulate a question that (only) the user can answer if he has forgotten his password.

Field label	Your input
Forgot answer	Provide the answer to the above password question.
SMS number	If the user is to receive an SMS in the event of an alarm or failure, provide his cell phone number. Please insert a full international number starting with a '+'. Example: +43 123 456 7890. Please note that an SMS sending device has to be connected to the VisoGuard server for this feature to work. Refer to the manual *Thecus VisoGuard 4.0 Server Installation and Administration* for information about supported devices and how to connect and setup them.
E-mail address	If the user is to receive an e-mail in the event of an alarm or failure, provide his e-mail address.
Language	Specify the preferred language for this user.
Auto login after 1 min timeout	Defines whether this user should be logged in automatically when nobody else logs at the login panel in for 1 minute. This option can be enabled for only one user at a time.
PTZ priority (1=lowest, 10=highest)	Defines the relative PTZ priority between users. A user with higher priority can take away PTZ control from a user with lower priority. Please note: The automated PTZ actions started by the event manager and scheduled routes have priority 4. Therefore users with priority 1 to 3 will be overridden by automatic PTZ actions, whereby users with priority 5 to 10 can override automatic PTZ actions but will not be interrupted by them.
Max. PTZ use time (sec)	Maximum allocation time, after which a PTZ camera is automatically released. Zero means no limit.
PTZ inactivity timeout (sec)	When a user has taken PTZ control and is inactive for a certain amount of time, the PTZ camera is freed automatically after this timeout. Zero means no timeout.

5. Push **Next** to go the **Privileges** dialog. Here set the privileges for the new user (see *4.2 Setting general user privileges* on page 30 for details).
6. Push **Next** to go the **Camera Access Rights** dialog. Here set the camera access rights for the new user (see *4.3 Setting camera access rights* on page 31 for details).
7. Push **Save** to create the new user account with the settings you entered.

4.2 Setting general user privileges

For each user and group certain privileges can be defined. These privileges define to which tools and data a user has access and what he can do.

1. Choose **User admin** from the **System administration** menu. This opens the **User admin** dialog.
2. Select the user or group you want to modify.
3. Click on the **Next** button to move to the **Privileges** dialog. Here you can edit privileges for the user or group. In their initial state, all privileges in this dialog are inherited from the upper group level. Inherited privileges from the group level to which the user or group belongs are displayed

with normal font, while values that you define at the current user or group level are displayed in **bold**.

Use the scroll bar to access the lower part of the list.

4. Choose **Modify selected user or group** from the menu.
5. Set the privileges according to your needs. To change a privilege click on its button and select the status from the pop-up menu (either **Inherited**, **Enabled**, or **Disabled**).
   To set privileges for all users in the system you can select and modify the root group (but please be aware that at each group or user level privileges can be overridden).
6. Push **Save** to save your changes.

4.3 Setting camera access rights

1. Choose **User admin** from the **System administration** menu. This opens the **User admin** dialog.
2. Select the user or group you want to modify.
3. Click the **Next** button twice to get to the **Camera Access Rights** dialog.

   Analog to the user privileges the camera access rights are inherited from the upper group level. Inherited access rights from the group to which the camera or camera group belongs are displayed with normal font, while values that are defined at the current level are displayed in **bold**.

4. Select the camera or camera group you want to look at or modify.
5. Choose **Modify selected user or group** from the menu.
6. Set the rights according to your needs.
   To set access rights for the selected user or group for all cameras in the system you can select and modify the root camera group.
7. Push **Save** to save your changes.

4.4 Working with user groups

User groups are a powerful means to manage and organize users. For instance, you can set privileges for groups that are then inherited by the users belonging to this group.

4.4.1 Creating a user group

1. Choose **User admin** from the **System administration** menu. This opens the **User admin** dialog.
2. In the list of users and groups, select a user group to which you want to add a new group.
3. In the menu select **Add new group** which will open the new group dialog that allows you to define a **Group name**.
4. Press Next to edit the group **Privileges**. The privileges are the same as for a user. Inherited privileges are displayed in normal font while privileges defined at this group (level) are displayed in bold font.
5. Press **Save** to create the new group.

4.5 Defining Online Monitor views for a new user

If a new user needs to work in the Online Monitor then camera views need to be defined. Generally, there are 2 ways for doing that:

- Login as the new user and manually create new views as described under *5.1 Creating a new view* on page 34, or

- copy existing views from another administration user as described under *5.8 Copying views between users* on page 41.

4.6 Information about logged-in users

VisoGuard allows you to get information about logged-in users:

1. Choose **Users...** from the **System administration** menu. Now you see the list of logged-in users with information about the host from which the user logged in, login time, total bytes transmitted since login, and bandwidth.

4.7 Changing the password

This section describes how to change passwords for users defined in VisoGuard. For users defined in Active Directory/LDAP, the passwords need to be changed there.

Each VisoGuard administrator with the appropriate privileges can change the passwords of other users (see also *4.1 Creating a new user account* on page 29).
Additionally, each user can change his own password by following these steps:

1. In the **VisoGuard** menu choose **Change password...**.
2. In the newly opened dialog enter the old (current) password and the new password twice.
3. Push **OK** to change the password. When you login the next time, you will have to enter the new password.

Please note: The optional secondary password can only be changed by an VisoGuard administrator with the appropriate privileges.

4.8 Working with users from Active Directory or LDAP

You can configure your VisoGuard server to import users from an Active Directory (AD)/LDAP server. In this case the users (user names and passwords) are maintained in AD/LDAP and users are imported (mapped) to a user group in VisoGuard. The privileges of these users (what they are allowed to do in VisoGuard) are defined at the VisoGuard user group where they belong to.

4.8.1 How VisoGuard and Active Directory/LDAP work together

When an connection to an Active Directory/LDAP server is set up correctly, VisoGuard imports users of a matched group in Active Directory/LDAP. These users are imported to a certain user group in VisoGuard. The privileges and camera access rights of the users imported from Active can be defined at the user group in VisoGuard.

When the VisoGuard server connects the Active Directory/LDAP server the first time, it loads all matched users into the user group in VisoGuard. These users are then cached in VisoGuard (no user passwords are stored in VisoGuard). Each 2 minutes the list of users is reloaded from the Active Directory/LDAP server.

Each time when a user that is defined in Active Directory/LDAP logs in to VisoGuard the password is checked (authenticated) with the Active Directory/LDAP server. This means that at login time an active connection to the Active Directory/LDAP server must be present.

Also note that no VisoGuard-specific information is stored in Active Directory/LDAP.

4.8.2 Setting up an Active Directory/LDAP connection

First you need to define a user group to which you want to import the AD/LDAP users:

1. Choose **User admin** from the **System administration** menu. This opens the **User admin** dialog.
2. In the user tree select a group that should serve as the container for the users imported from AD/LDAP. The group must be empty, it must not contain any local users.
   If you do not have an appropriate group, you can create a new user group by selecting the parent group under which you want to create the new user group. Then choose **Add new group** from the menu, supply a name, and push **Save**.
3. Choose **Modify selected user or group** from the menu.
4. Select the check box **Users of this group are imported from Active Directory**.
5. Now you can define the privileges and camera access rights of the imported users by going to the **Privileges** dialog and the **Camera access rights** dialog (push the **Next** button to move to these dialogs).
6. Push **Save**.

Once you have enabled a group for AD/LDAP import you must setup the connection to an AD/LDAP server:

1. Choose **Active directory configuration** from the menu. This opens the **Active directory configuration** dialog (this dialog actually is part of the **Host admin** dialog). In this dialog you can
   - define the connection to an AD/LDAP server
   - define an AD/LDAP filter to match a certain AD group (set of users) for importing to VisoGuard
   - define the Tag mapping between AD/LDAP and VisoGuard
2. Choose **Modify host** from the menu.
3. Under **Connection parameters** define the filters for matching a certain AD group (set of users) for importing to VisoGuard.
   Under **Observer group name** you must enter the name of a user group in VisoGuard for which you enabled the **Users of this group are imported from Active Directory**. Please note that AD servers usually can be accessed at **Port** 389.
   With **Test connection** you can check whether the server can be accessed with these values.
4. Under **Directory parameters** define the AD/LDAP filters to match a certain AD group (set of users) for importing to VisoGuard. The filter fields **Search base**, **AD group name**, **Directory address** are available for further constraining the matched user group in AD and need to contain the fully qualified strings in AD (e.g. OU=Video-users, DC=netavis, DC=net).

   In **Observer group name** please add the name of the VisoGuard group where the users are to be imported.

   Select or create the appropriate **Attribute mapping schema**. The attribute mapping defines what AD attributes are mapped to which VisoGuard attributes. Usually these are the mappings:

   For Active Directory:

Attribute	Value
Login name tag	cn
Name tag	displayName
SMS number tag	telephoneNumber
Email tag	mail

   The **Tag mapping** defines further attribute mappings. For Active directory the **AD group identifier tag** must be set to `memberOf` and **Login name tag** must be set to `cn`.

5. Push **Save**.

Now the users from AD/LDAP should be imported to the specified user group in VisoGuard.

5 Using the Online monitor

In the **Online monitor** you can view live streams from cameras that are set up at the VisoGuard server. The prerequisite is that you must have authorization to access the Online Monitor (see *4.2 Setting general user privileges* on page 30). Furthermore, you can access only those cameras for which you have access rights (see *4.3 Setting camera access rights* on page 31).

When a new user logs in the first time he will encounter an empty Online monitor waiting for new camera views to be defined. Once you have defined your views they will reappear next time you log in.

You can also have several Online monitors in multiple windows (see *2.4 Client multi-window and multi-screen operation* on page 17).

Important: If you are using a low-bandwidth connection between client and server (e.g. via wide area networks) it can happen easily that the video streams cannot pass through the connection fast enough, which results in bad frame rates and slow responsiveness of the client. In such a case you should use the Transcoding™ feature of VisoGuard. See *2.5 VisoGuard Transcoding™ for low-bandwidth client-server connections* on page 19 for further details.

5.1 Creating a new view

VisoGuard lets you create an unlimited number of named views. Each of these views can contain up to 100 camera view ports.

1. Choose **Create new view** (either from the empty Online monitor or from the **Control menu**) to open the **Create new view** dialog.
2. You can now choose the layout for your view from predefined templates and you also can define an arbitrary matrix of up to 10 x 10 views. A new dialog is opened asking for the name of the view and the aspect ratio for the view ports.

   The **Name of view** is shown in the view selector at the top of the screen. Please note that you can also create a view hierarchy by using colons ":" between the names. In the example above we create a new view in the group called "Main Building" with a name "First Floor". There might also be a view called "Second Floor" or "Third Floor".

   The **Aspect ratio** pop-up defines the aspect ratio of the view ports in the view:

   - Fixed aspect ratios: PAL, NTSC, VGA, double VGA, or HDTV 16:9.
   - **Fill available space**: This is the default setting and will adapt the view port size (and hence the aspect ratio) to fill the available space.
   - **Custom aspect ratio**: here you can freely define an N:M aspect ratio.

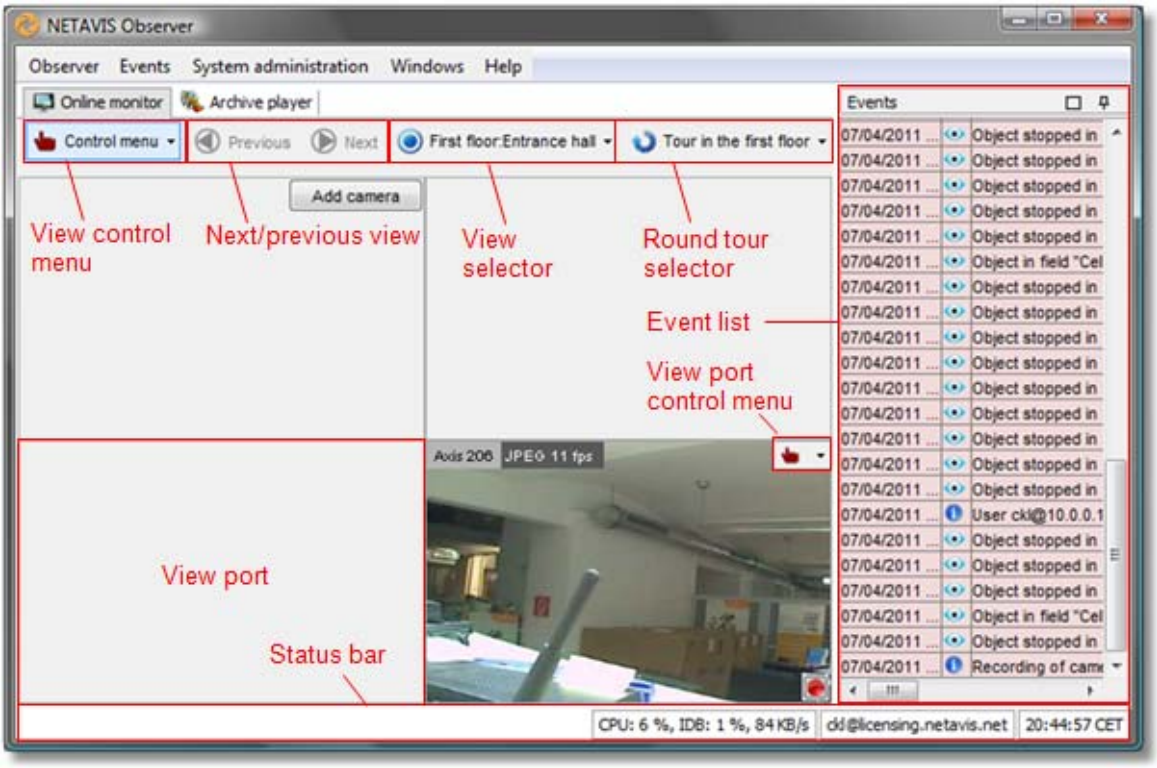
   The setting **Stretch image to fit into view port** (selected by default) defines whether a camera image can be stretched to fit into the view port. This may cause distorted images for aspect ratios that do not fit the current view port aspect ratios.

   The setting **Crop image to fit into view port** defines whether a camera image can be cropped to fit into the view port. This may cause that some parts of the image are not visible in the view port. In the section *5.4 Modifying view port settings* on page 37 you can define what part of the cropped camera image is to be shown in the view port.

   Please select an aspect ratio that fits most of your cameras you plan to show in the view. Selecting an improper aspect ratio can lead to unused space on the screen.

   Press **OK** to acknowledge your input.

3. In accordance with the selection above, VisoGuard creates a new view that might look as follows (your view may have a different number of view ports depending on what you selected):



The view ports fill the central part of the window, and each view port has its own view port controls.

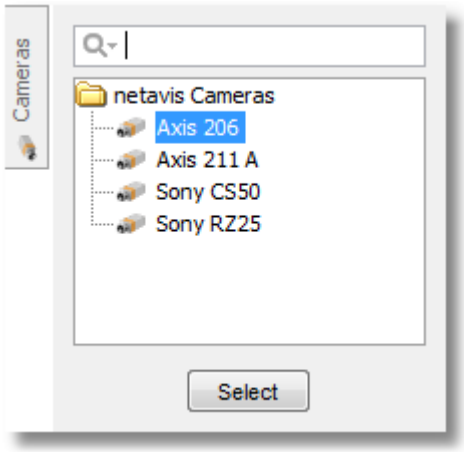
At the right side of the window is the **Event list**, which is explained in *8 Handling events* on page 61.

4. Choose **Save all view settings** from the menu in order to save all settings for your current user. The next time you log on to VisoGuard, all views will then be available again.If you neglect to save, all changes are lost when you exit the application.

Please note: All view settings will be stored, also quality and fps settings of view ports. New views will be stored automatically without the need to save manually.

5.2 Selecting cameras

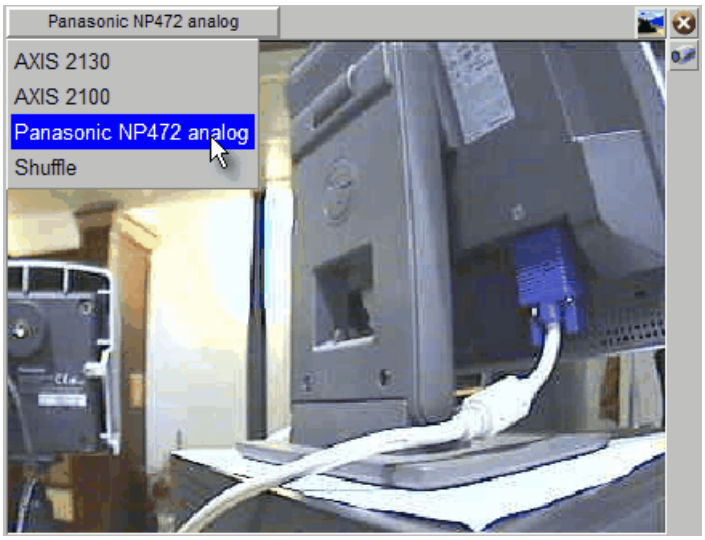
1. In the view port push the **Add camera** button. Please note that you first have to set up a camera before you can select it in one of the view ports (see *3 Setting up cameras* on page 20). This opens the camera tree.
2. Select a camera from the newly opened camera tree.



You can either:

- select a camera push the **Select** button or
- double click on a camera to add it to the view port where you pushed **Add camera** or
- drag and drop a camera to the view port of your choice

3. Proceed in the same way with additional view ports in your view.
4. You can assign multiple cameras to each view port. However, since you can only view one camera image in each view port, VisoGuard lets you manually switch between cameras by clicking on the camera selection menu at the upper left corner of the view port.



5. In the camera selection menu of a view port you can also select the option **Shuffle**. Then VisoGuard cyclically switches through all the cameras assigned to the view port.
6. Please select **Save all view settings** from the view **Control menu** in order to save all settings. The next time you log in to VisoGuard, all views and view ports will be available again.

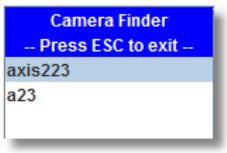
5.3 Navigating in the Online monitor

You have several options for navigating in the Online monitor:

- Select a view from the **View selector** pop-up.
- Select a Round tour from the **Round tour selector** pop-up.
- Use the **next/previous view** buttons to navigate to the previously displayed views.
- Double click in a view port to get a big view of the actually displayed camera in the view port. If there is a view defined containing a big view port with the camera, then this view will be

exposed. Otherwise a new temporary view with the camera will be created. You can then go back to the previous view by pushing previous view button.

- Use the quick **Camera finder**: You can just start typing at your keyboard. A little **Camera finder** pop-up will show at the lower right corner of the client window and will show a list of cameras with matching names and ids:



You can double click a camera or select it with the keyboard and press **ENTER**, which will expose a big view of the camera (which is the same action as a double click in the view port). The behavior of the action can be customized (see document *Thecus VisoGuard 4.0 Server Customizing*).

5.4 Modifying view port settings

VisoGuard allows you to set various options including video quality of either single view ports or all view ports in the current view at once.

The settings of a single view port can be modified via the view port's control menu that appears in the upper right corner of a view port when you move the mouse pointer over the view port.

The view port control menu offers the following options:

5.4.1 Adding and removing cameras

Cameras can be added and removed with the **Add camera** and **Remove camera** menu entries. Please refer to section *5.2 Selecting cameras* on page 35 for more details.

5.4.2 Controlling PTZ cameras

The **PTZ** menu allows PTZ control and is enabled for PTZ cameras (see *9.4.1 Controlling PTZ cameras in the Online monitor* on page 67).

5.4.3 Setting video parameters

The **Set video parameters** menu offers the following options:

Set streaming format	defines how the camera images should be streamed. The available options depend on your camera and your setup of the cameras inside VisoGuard (see *3.2 Adding a new camera and setting basic properties* on page 20). Please refer also to *1.4 Video streaming methods and compression* on page 6 for further details on streaming formats.
Set image quality	sets the quality of the streamed images by modifying the compression rate. The options are **High**, **Medium** and **Low**. Refer to *1.4.5 JPEG image sizes and storage requirements* on page 8 for details on these values.
Set image size	sets the image size of the streamed images. The available size options are camera-specific. Please refer to your camera's manual. Please note that for MPEG cameras you cannot change the size of streamed images. The sizes of streamed MPEG
Set frame rate	sets the frame rate of the video stream. The options are **Max fps**, **various fps and fpm values** and **Stop**.

Set camera name appearance	defines the position where the camera name is displayed in the view port.
Rendering preference	defines which scaling algorithm will be used when images need to be scaled to fit the available view port space. In the **Optimized for speed** means that the scaling is done with a faster algorithm that may cause lines to be not so smooth. **Optimized for quality** means that the scaling is done with a more CPU-intensive anti-aliasing which causes straight lines to be smoother.

These settings can be modified all at once for all view ports in the current view via the **Set parameters of all view ports** from the view **Control menu**. Holding down the **CTRL** key while selecting any of the **Set parameters of all view ports** commands will modify all view ports of all views (not just the current view).

5.4.4 Controlling video analysis (iCAT) display

The iCAT menu offers various options for displaying iCAT-related video analysis information. Please refer to *14.4 Working with iCAT* on page 113 for further information.

5.4.5 Defining a crop area

For views where you have the **Crop image to fit view port** setting selected, you can define what part of the cropped camera image you want to see by choosing **Define crop area...** from the menu.

5.5 Zooming in a view port and in archive recordings

VisoGuard allows you to zoom view ports in the Online monitor and in the Archive player.

Basically, you have two ways to zoom a view port or a recording in the Archive player:

5.5.1 Zooming with the mouse wheel

1. Just move the mouse pointer over a view port and turn the mouse wheel. The view port will zoom accordingly.
2. You can move the zoomed area in a view port by dragging it with the mouse.
3. Use the mouse wheel again to zoom out.

5.5.2 Zooming by drawing a zoom rectangle

1. With the mouse draw a rectangle in a view port.
2. Click in this rectangle, which will cause the view port to zoom accordingly.
3. You can position the zoom by dragging the rectangle. You can also modify its size by turning the mouse wheel.
4. Click outside the rectangle to return to normal (not zoomed) view.
5. You can remove the zoom rectangle by clicking into it with the mouse and pressing the **Delete** or **Backspace** key. Alternatively, you can drag the rectangle outside of the view port to remove it.

   You can also have multiple zooming rectangles per view port.

Showing a zoomed view in another view port (Online monitor only)

1. Draw a zoom rectangle with the mouse.
2. Click into another view port. Now the zoomed area is shown in the other view port.
3. You can position the zoom by dragging the rectangle.

4. You can remove the zoom by clicking the rectangle with the mouse and pressing the **Delete** or **Backspace** key. Alternatively, you can drag the rectangle outside of the view port to remove it. Removing a rectangle will also remove the zoomed view from the other view port.

Please note: When PTZ control is enabled, any mouse actions are taken for PTZ control. In order to control the view port zooming, hold down the **CTRL** key while using the mouse.

5.6 Manual recording control in the Online Monitor

In addition to programmed recordings, you can also manually start and stop continuous recordings directly in the Online monitor. When manual recording control is set up, a recording button is shown in camera view ports in the Online monitor.

5.6.1 Setting up manual recording control

To enable recording control, you must do 2 things:

- Enable the manual recording camera access right for the user
- Set up a continuous recording schedule for the camera. The continuous recording schedule that is active at the time when the user pushes the manual recording button defines the format of the recording. Therefore you can also have different manual recording formats for different times in the day or week.

Enable the manual recording camera access right

Here is how to set the camera access right for manual recording (see *4.3 Setting camera access rights* on page 31 for a general description on how to set camera access rights):

1. Login as administrator user (or another user with the right to modify user data).
2. Choose **User admin** from the **System administration** menu. This opens the **User admin** dialog.
3. Select the user or group for which you want to enable manual recording control.
4. Click the **Next** button twice to get to the **Camera Access Rights** dialog.
5. Select the camera or camera group for which you want to enable manual recording control.
6. Choose **Modify selected user or group** from the menu.
7. Enable the right **Manual recording control from Online monitor** by choosing **Enabled** from the pop-up menu.
8. Push **Save** to save your changes.

Set up a continuous recording schedule

In order to use manual recording control for a camera you have to define a continuous recording schedule (please refer to *6.1.1 Programming continuous timed recordings* on page 43 for a general description of setting up schedules for continuous recordings):

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. In the camera tree select the camera for which you want to set up the recording schedule.
3. At the bottom of the screen, click on the **Next** button twice. This takes you to the **Scheduling** dialog. If you are setting up a new camera, this dialog will be quite empty.
4. In the menu select **Modify selected camera or group**.
5. Click the **Add** button to add a schedule slot to the **Time Intervals** list.
6. Click the **Change** button and choose **Continuous recording**.
   Now the **Scheduling** dialog shows the settings for configuring continuous recording.

7. Now you can define the days and times for the recordings. You can activate individual days or, with the **All** button, the whole week at once. Select hours and minutes from the popup matrix. If you want that recording can only be started manually then make sure that the **Enable interval** checkbox is disabled.

   Note: When a user pushes the manual recording button in the Online monitor actually the **Enable interval** checkbox is toggled. This causes the recording to either start ort stop.

8. Set all the recording options as described in *6.1.1 Programming continuous timed recordings* on page 43.
9. Click on **Save** to save your settings.

5.6.2 Manually controlling recordings in the Online monitor

When everything is set up as described above then for the enabled user and camera a manual recording button is shown in any view port displaying the camera.

You can switch recording on and off by pushing the manual recording button. The recording state is shown by the color (a strong red dot means recording is on, otherwise recording is off).

Please note: For times not covered by a continuous recording schedule no manual recording button is shown.

5.7 Working with round tours (the Smart guard™ function)

VisoGuard allows you to make virtual round tours of views. You can define round tours that contain certain views. When a tour is started, VisoGuard walks you through all the views by automatically showing up the views in the **Online monitor**. This is like a virtual patrol of a security guard (Smart guard™ function).

5.7.1 Defining a round tour

Steps to add a new round tour:

1. Choose **Round tours…** from the view **Control menu**. Now the **Round tours** dialog opens.
2. In the **Round tours** dialog push the button **Add new round tour**.
3. In the **Tour name** field enter the name of the round tour.
4. Now you can select a view from the **Views** list and push the button to include it in the tour. By pushing the button you can remove a view from the tour. You reorder views in the tour by pushing the **Up** and **Down** buttons.

   Please note: You can have the same view several times at different locations in a round tour. You can select multiple views in the **Views** list at once by holding the **CTRL** key while selecting the views.

5. For each view you can set a **Shuffle duration** that determines, how long (in seconds) this view is shown before VisoGuard automatically changes to the next view in the tour. By pushing **Set for all** you can set the same duration for all view in the round tour.
6. Push **Save** to save your changes and **OK** to leave the dialog.

Later on you can modify an existing round tour by opening the **Round tours** dialog and then choose an existing round tour from the **Round tours** list and push **Modify round tour**.

A tour can be deleted by opening the **Round tours** dialog and then choose an existing round tour from the **Round tours** list and push **Delete round tour**. Then you have to enter your password to confirm the delete.

5.7.2 Working with round tours: The Smart guard™ function

After you have defined a round tour, a new **Round tour** selector appears in the **Online monitor**. To activate the round tour, just choose its name from the **Round tour** selector. This activates the automatic walkthrough all of the views in the round tour (Smart Guard™ function). The name of the round tour now appears in green to show that it is active. You can stop the tour by choosing a view from the **View** selector (the **Round tour** selector will change its color to normal to show that no tour currently is active).

5.8 Copying views between users

If there are several users in a system it can be a lot of work to create views for each user individually. In order to help, VisoGuard offers the possibility to copy complete views (including all view settings) or even all views of an administrator user to another user. Important is that the user who copies the views to other users must have user administration rights („User admin: Access to User administration“ and „User admin: Manipulate user data“).

Here is how you can do that:

1. Login as the user from whom you want to copy the view(s) and go to the Online monitor.
2. Create/define the view(s) you want to copy. Please note that only saved settings are copied.
3. Select the view you want to copy and then choose **Copy current view to other users…** from the view **Control menu**. Now a user selection dialog opens.
4. Select the users to whom you want to copy the current view. Multiple users can be selected by holding down CTRL while clicking on user names. After you have finished selecting the users, press the **Select** button. Now the selected users receive a copy of the current view.

You can also copy all views of the current user by choosing **Copy all views to other users…**
If the users already have views with the same name as the copied views, then the existing views will be overwritten by the copied ones!

Please note: The user, who was copied to has to login again in order to see the newly copied views.

5.9 Working with MPEG cameras and audio (MPEG-4, H.264, and MxPEG)

Note: In the current version of VisoGuard, MPEG and bidirectional audio is only supported by clients running on MS Windows. For further details please refer to *2.1 Introduction the VisoGuard client* on page 10.

VisoGuard also supports MPEG cameras (MPEG-4, H.264, and MxPEG) with audio streaming (see also *3.2 Adding a new camera and setting basic properties* on page 20).

If the camera allows MPEG streaming, you can select the MPEG streaming format from view port control menu. Once the MPEG streaming is activated, additional MPEG controls appear on the view port(s):

These controls allow you to see and modify Audio aspects:

Audio from the camera: indicates that audio from the camera is on. indicates that audio from the camera is off. A click on the icon turns it on or off.

Audio to the camera: indicates that audio from your microphone to the camera is on. indicates that audio from your microphone to the camera is off. A click on the icon turns it on or off.

If you have the **Default settings** in the **Camera Admin** set to **Audio from and to share single button** then you will see only one control icon: **Bidirectional Audio**: indicates audio in both directions is on (loudspeaker and microphone is on). indicated that audio in both directions is off (loudspeaker and microphone is off).

6 Working with archive recordings

This section shows you how to work with the VisoGuard recording archive, particularly in the following areas:

- Programming archive recordings (timed or triggered by iCAT (video analytics) events)
- Selection and playback of archive recordings

Please note: In order to work with archive recordings you need to have the appropriate user privileges and camera access rights (for further details see *4.2 Setting general user privileges* on page 30 and *4.3 Setting camera access rights* on page 31).

6.1 Programming archive recordings

Two types of programming are available in VisoGuard:

- timed recording
- recording on iCAT (video analysis) events like motion detection or people counting

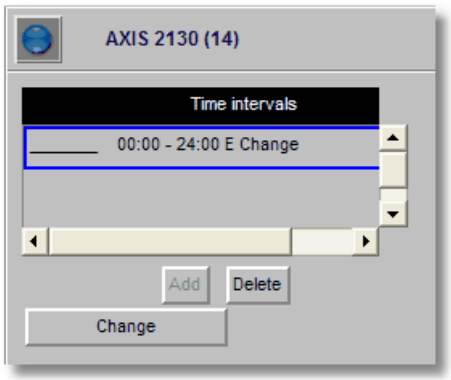
To be able to program recordings, you need corresponding authorization.

6.1.1 Programming continuous timed recordings

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. In the camera tree select the camera for which you want to program archive recording. When you select the camera (highlighted in light blue), its data are displayed in the **Properties** dialog at the right side of the screen.
3. In the menu select **Modify selected camera or group**.
4. At the bottom of the screen, click on the **Next** button twice. This takes you to the **Scheduling** dialog. If you are setting up a new camera, this dialog will be quite empty.

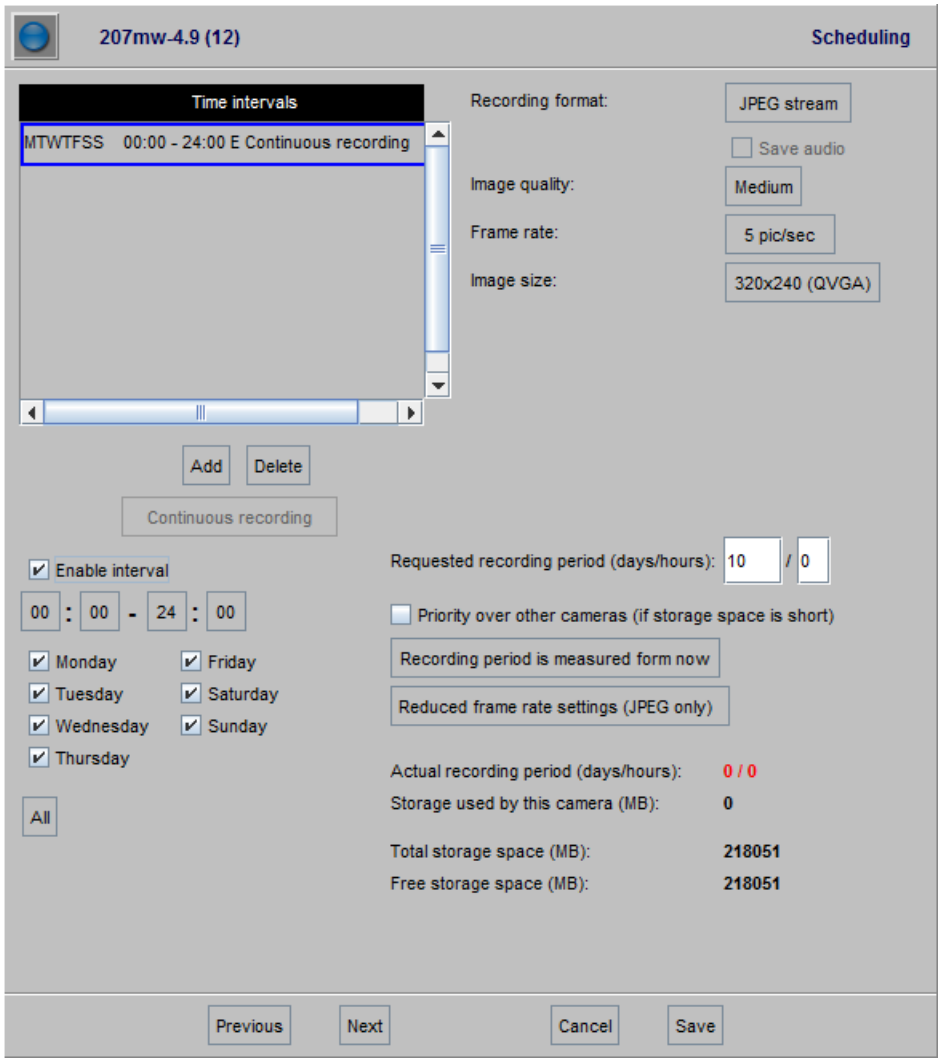
   Note: some fields and buttons are deactivated. Only when you select **Modify selected camera or group** in the menu they become editable.
   Also, the **Time Intervals** field is still empty when you begin. Later it will contain one or more program slots for the selected camera.

5. Click the **Add** button to add a programming slot to the **Time Intervals** list.



   The new entry will be selected.

6. Click the **Change** button (now enabled) and choose **Continuous recording**.
   Now the **Scheduling** dialog shows the settings for configuring continuous recording:



7. Now you can define the days and times for archive recordings. You can activate individual days or, with the **All** button, the whole week at once. Select hours and minutes from the popup matrix. Please make sure that the **Enable interval** checkbox is marked, because only then are the settings enabled and recording is started.

   Note: If you want to record at different times on different days, you can create multiple recording intervals. For each recording interval proceed as described here.

8. In addition to defining the weekdays and times, you need to specify the **Recording format**. If your camera also supports multiple formats you have several choices (for details on streaming formats please refer to *1.4 Video streaming methods and compression* on page 6):

   - **JPEG stream** is also known as MJPEG, where the server stores sequences of JPEG images.
   - **MPEG-4 video** for MPEG-4 video streams.
   - **H.264 video** for H.264 video streams.
   - **MxPEG video** for MxPEG video streams.

   For the MPEG video formats you can additionally select **Save audio**.

   When you choose any of the MPEG video formats then the video settings that are defined in the camera's Default settings will be taken for recording (*3.2 Adding a new camera and setting basic properties* on page 20).

If you choose **JPEG stream** you can additionally set the **Image quality**, the **Frame rate** and the **Image size** for the archive recording:

Set the values according to your needs. See *1.4.5 JPEG image sizes and storage requirements* on page 8 for details on images sizes, quality, and storage requirements.

Note: Some cameras are only capable of a single picture stream which will constrain the possibility of recording in multiple formats and having different video stream settings in the Online Monitor and the recording. Please refer to the document *Thecus VisoGuard 4.0 Supported Video Sources* for information about supported cameras and their streaming capabilities.

9. Fill in the **Requested recording period** for this camera. This value defines how long VisoGuard will keep recordings. Recordings that are older than **Requested recording period** the will be automatically deleted by VisoGuard (see also *6.1.3 Operation of the VisoGuard dynamic storage management* on page 45).
   You can also select **Priority over other cameras (if storage space is short)** to give this camera priority over other cameras if the available storage space is too short for all requested recordings of all cameras (for further details see *6.1.3 Operation of the VisoGuard dynamic storage management* on page 45).
   You can also define what the requested recording period refers to: either **Recording period is measured from now** or **Recording period is measured from youngest recording**. There can be quite a difference between these two choices for the following case: Assume a motion detection-based recording that only triggers recording once every few weeks.

   Optionally, in order to save disk space, you can lower the frame rate of older parts of the archive. To do that click on **Reduced frame rate settings (JPEG only)...** to open a small dialog that allows you to enter a reduction period and a reduced frame rate.
   For example, setting 30 days of **Requested recording period** with 25 fps and 20 days for reduced archive with 3 fps will maintain an archive containing recent 10 days with 25 fps and the remaining 20 days will be automatically reduced to 3 fps.
   Please note that this works for JPEG streams only and does not affect any MPEG recordings.

   Additionally, you can see the **Actual recording period (days/hours)**, the **Storage used by this camera (MB)**, the **Total storage space (MB)** which shows the overall storage space of the server, and the **Free storage space (MB)** which is the available space for new recordings on this server.

10. Click on **Save** to save your settings. As soon as the scheduled time is reached recording is started with these settings.

6.1.2 Scheduling video analysis (iCAT) operation and recording

For information on how to schedule video analysis (iCAT) operation and recording please refer to section *14.3.9 Scheduling iCAT operation and recording* on page 110.

6.1.3 Operation of the VisoGuard dynamic storage management

In the **Scheduling** dialog you can specify the **Requested recording period** property that defines how long recordings are to be kept by VisoGuard. Any recordings that are older than the requested recording period are automatically deleted as long as you do not manually protect them from deletion (see *6.2.8 Protection of recordings against automatic deletion* on page 51).

For cases like motion detection-based recording it can be very difficult if not impossible to estimate the required storage space and therefore space for all requested recordings could be too short. To help with this hopefully rare case, VisoGuard uses an intelligent storage management process. This process always tries to store all requested periods for all recorded cameras.

However, if there is not enough space available, the allocation process is doing two things:

- It generates a system event once a day and sends an email / SMS to the VisoGuard administrator telling him that there is not enough space for all recordings.
- It automatically truncates the recordings of cameras to allow a proportionally even distribution of the available space among all cameras.

For some special cameras that have to record the requested storage period in any circumstances, VisoGuard offers the **Priority over other cameras (if storage space is short)** flag. If this flag is set for a camera, VisoGuard always tries to store the requested period for this camera and truncates other cameras that do not have this flag set a little more. If there is more than 1 camera that has the flag set, the storage management process tries to store all of those cameras.

Algorithm of the dynamic storage management process:

Fill-time-percentage (FTP) = 100 * Actual-recording-time / Requested-recording-time.

VisoGuard tries to keep the FTP of all cameras of each of the two priority classes the same (high-priority cameras and lower-priority cameras). First the algorithm tries to fully record the high-priority cameras and then use what is left for the lower-priority ones, whereby all of those will reach the same FTP. However, the low priority cameras can never go below an FTP of 10%. If the low priority cameras reach a level of 10%, then the storage management process starts truncating the archives of the high priority cameras as well. Anyway, this should never happen in a normal case and is only possible if the storage space is totally insufficient for holding the programmed recordings.

Since the storage management process considers recording time and not recording space for distributing the available space, it happens that the relatively small recording space of a camera with a low recording frame rate is truncated in the same proportion like the relatively big recording space of a camera with a high recording frame rate.

Caution: Please be careful when you set the **Priority over other cameras** flag since, if storage space is short, VisoGuard truncates the archives of all other cameras in favor of this camera. If available storage space is much too short relative to the requested storage periods of all cameras, this can lead to strongly truncated archives.

6.2 Playback of archive recordings

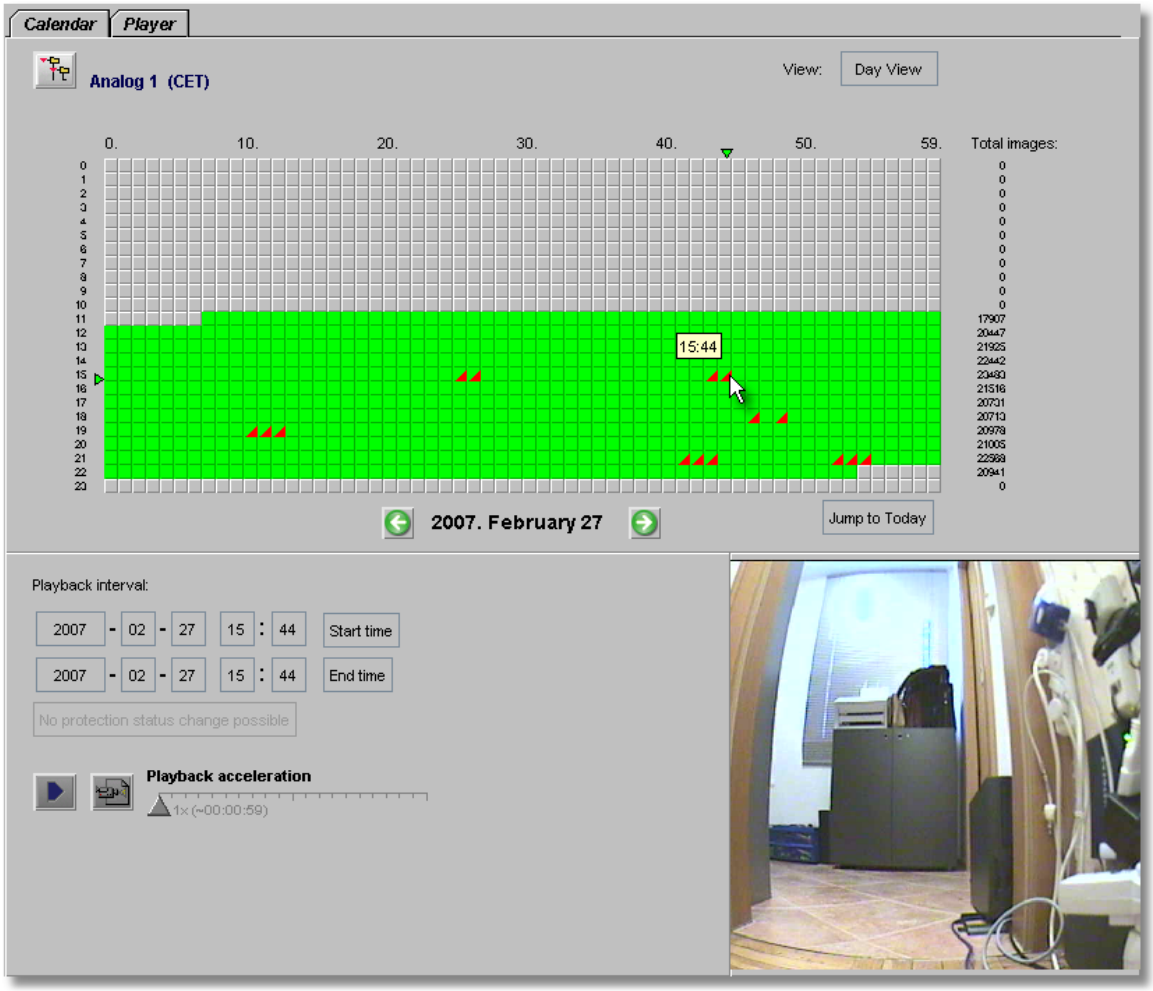
VisoGuard features a multitude of powerful functions for working with archives.

6.2.1 Selecting the camera and the playback period

1. Go to the main window and choose the **Archive player** (if the Archive player is not available, then perhaps it is disabled in the client preferences; see *2.4 Client multi-window and multi-screen operation* on page 17).

   Either the **Camera tree** appears immediately or you have to push the **Select camera** button :

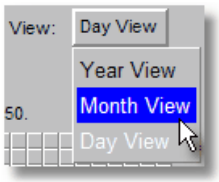
2. Select the camera from the camera tree and push **Select** (you can also double click a camera or drag it to the calendar view). An overview for the selected camera on the current day is displayed:



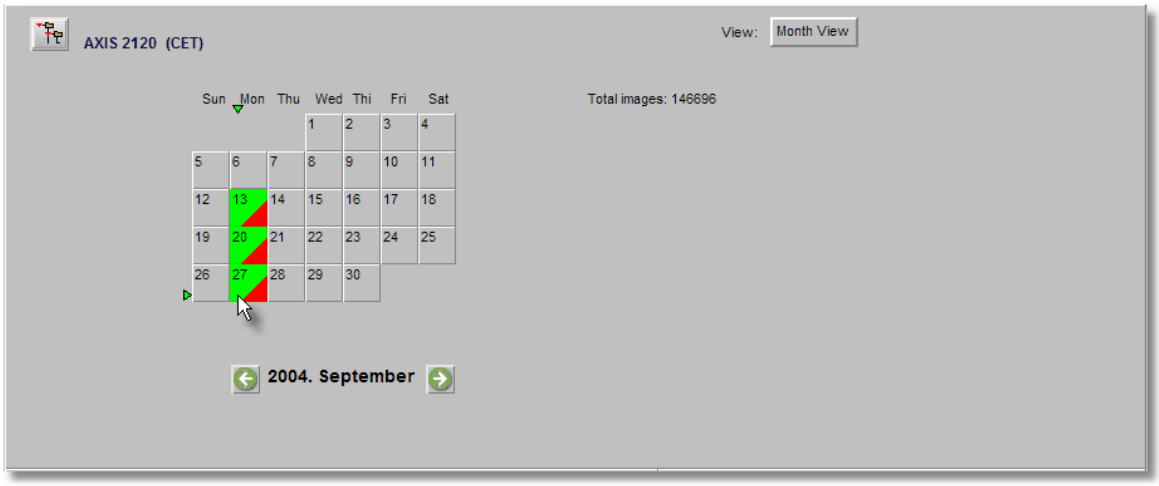
This one-day overview shows green blocks indicating minutes for which recordings have been archived. A red corner in a block indicates that an event was triggered and an event recording was started in that minute.

When you move the mouse pointer over a green block, then the first recorded frame of this minute is displayed in the lower right corner of the window.

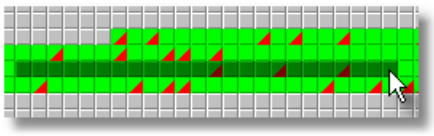
You can also switch to a monthly or an annual overview via the **View** button and its popup menu.



Here is an example of a month view for the camera:



3. With the mouse select the time span of the archive that you want to play back. To do this press the left mouse button at the start of the time range, then move the mouse pointer to the end of the time range and then release the mouse button. The color of the selected time range changes to dark green.



4. Also select the playback acceleration by moving the **Playback acceleration** slider (default value is 1). At the slider you can see in parentheses how long the selected time will need for playback at the selected playback acceleration.
5. Now click the **Playback** button . This brings you to the **Player** view and the images for the selected time span are loaded from the server and then will be replayed with the specified acceleration (you can cancel the loading process by pushing the **Cancel** button).

In the **Playback view** you have several possibilities:

- Automatic or manual fast forward and rewind of recordings
- Selection and playback of a time frame (time zooming)
- Synchronous playback of recordings of up to 4 cameras
- Export of individual images as well as the selected video sequence

6.2.2 Moving forward and back in the recording

Automatic playback: By clicking the **Playback** buttons or you can let the recording automatically play forward or back. With the **Playback Speed** slider at the left of the window you can vary the playback speed. Press the **Stop** button to end playback.

Manual playback: By clicking and moving the green Playback marker , you can control the playback of images manually.

You can select the size of the playback by clicking the **Original size** button at the lower left of the **Player** dialog. Here you have the possibility to choose from various sizes.

6.2.3 Zooming in a view port and in archive recordings

VisoGuard allows you to zoom view ports in the Online monitor and in the Archive player.

Basically, you have two ways to zoom a view port or a recording in the Archive player:

Zooming with the mouse wheel

1. Just move the mouse pointer over a view port and turn the mouse wheel. The view port will zoom accordingly.

2. You can move the zoomed area in a view port by dragging it with the mouse.
3. Use the mouse wheel again to zoom out.

Zooming by drawing a zoom rectangle

1. With the mouse draw a rectangle in a view port.
2. Click in this rectangle, which will cause the view port to zoom accordingly.
3. You can position the zoom by dragging the rectangle. You can also modify its size by turning the mouse wheel.
4. Click outside the rectangle to return to normal (not zoomed) view.
5. You can remove the zoom rectangle by clicking into it with the mouse and pressing the **Delete** or **Backspace** key. Alternatively, you can drag the rectangle outside of the view port to remove it.

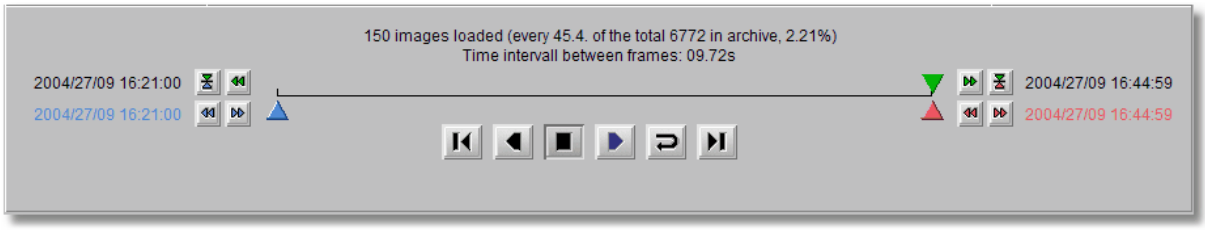
   You can also have multiple zooming rectangles per view port.

Showing a zoomed view in another view port (Online monitor only)

1. Draw a zoom rectangle with the mouse.
2. Click into another view port. Now the zoomed area is shown in the other view port.
3. You can position the zoom by dragging the rectangle.
4. You can remove the zoom by clicking the rectangle with the mouse and pressing the **Delete** or **Backspace** key. Alternatively, you can drag the rectangle outside of the view port to remove it. Removing a rectangle will also remove the zoomed view from the other view port.

Please note: When PTZ control is enabled, any mouse actions are taken for PTZ control. In order to control the view port zooming, hold down the **CTRL** key while using the mouse.

6.2.4 Playback of a time frame (time zooming)



1. The red and blue markers let you select a smaller time interval for detailed playback. Alternatively, you can click the **Set Blue Marker** button or **Set Red Marker** button to set the respective marker at the current position of the green Playback marker.
2. Click the **Zoom in** button to load and replay the time interval between the blue and red markers.

6.2.5 Playback with audio

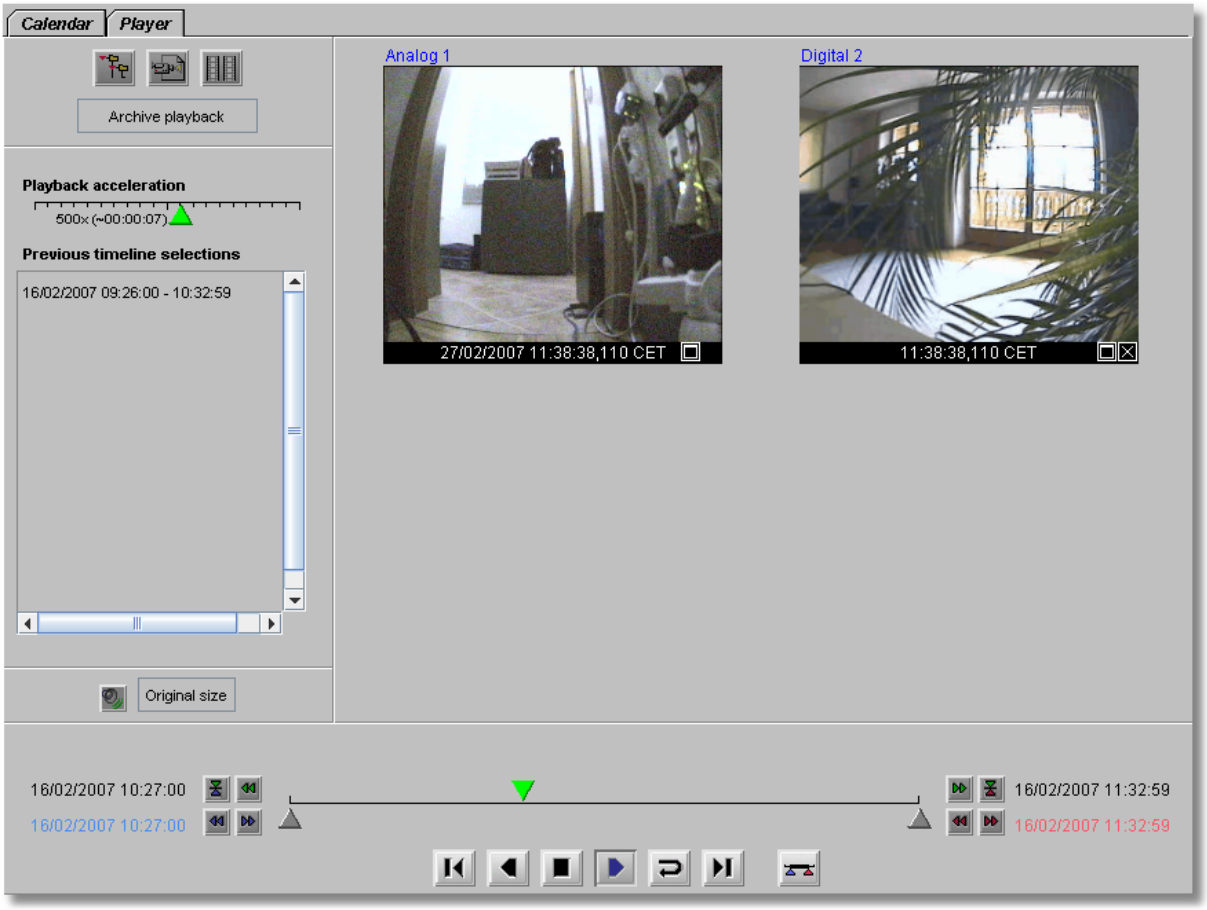
If the recording also includes audio (i.e. the recording has been done with MPEG-4 or H.264 and with Audio recording enabled), then you can decide whether you also want to replay audio. By default Audio is switched on, when you replay. To toggle audio on or off, push the button in the Playback view.

6.2.6 Synchronous playback of up to four recordings

1. Select the playback time frame for the first camera as described above. Then change to the **Player** view.

2. Click the **Synchronous Playback** button , which opens the **Camera tree**, where you can select the second camera for synchronous playback.
3. Repeat camera selection until you have up to 4 cameras for synchronous playback.

The following illustration shows synchronous playback of two cameras:



6.2.7 Displaying video analysis (iCAT) information for recordings

Th the **Control menu** the **iCAT** menu offers various options for displaying iCAT-related video analysis information also for recordings. Please refer to *14.4 Working with iCAT* on page 113 for further information.

6.2.8 Protection of recordings against automatic deletion

Normally VisoGuard automatically deletes recordings that are older than the **Requested recording period** in order to free space for new recordings. For cases where you want to keep certain scenes longer than the requested recording period you can protect arbitrary periods against automatic deletion. Here is how you can do that:

1. In the **Archive** go to the **Calendar** view and select a camera.
2. In the calendar select the period you want to protect against automatic deletion.
3. Press **Protect selected images against deletion**.
   Now the color of the selected period in calendar turns to a different color which shows that the images are protected.

To unprotect a protected period you must select this period in the **Calendar** view and Press **Unprotect selected images**.

Caution: Please be careful when using this feature since the protected recording periods will never be deleted automatically by VisoGuard. This means that the space will be locked as long as you keep them protected.

6.3 Exporting recordings (images and video sequences)

VisoGuard allows you to export individual images and video sequences in various formats.

With the SAFE format you can also export synchronous video sequences of up to 16 cameras simultaneously.

6.3.1 Exporting a single JPEG image (the current frame)

1. In the **Archive**, select a camera for the export.
2. In the **Player** view or in the **Calendar** view click the **Export** button to open the **Export** dialog.
3. Choose **Current image (JPEG)** from **Export format**.
4. Enter a file name for the image to be saved.
5. Mark the first checkbox if you want to overwrite a file of the same name that might exist.
6. When you click **OK** a file dialog will be opened asking where on your client computer you to want to save the file. Select the location and confirm.
7. Now you can use the exported file.

6.3.2 Exporting an archive recording in AVI DivX format

1. In the **Archive player**, select a camera for the export.
2. In the **Player** view or in the **Calendar** view click the **Export** button to open the **Export** dialog.
3. You have two **AVI** options for **Export format**:
    - **AVI (all images)**: This exports a video sequence with all the frames of the currently selected time frame (regardless of the **Playback acceleration** setting).
    - **AVI (Subsampled movie)**: This exports the time-lapse playback with the settings of the **Playback acceleration** slider. E.g. if you have selected a **Playback acceleration** of 3, your exported file will be roughly a third of the size of an **AVI (all images)** export. See also *6.2.1 Selecting the camera and the playback period* on page 46.
4. Enter the file name of video to be exported.
5. Mark the first checkbox if you want to overwrite a file of the same name that might exist.
6. When you click **OK**, a file dialog will be opened asking where on your client computer you to want to save the file. Once you select the location and confirm, a **File download progress dialog** will show the state of the export. You can cancel the export anytime by pushing **Cancel**.

Note: To play back exported video sequences with Microsoft Media Player, you need the DivX codec. You can download this for free from www.divx.com/divx.

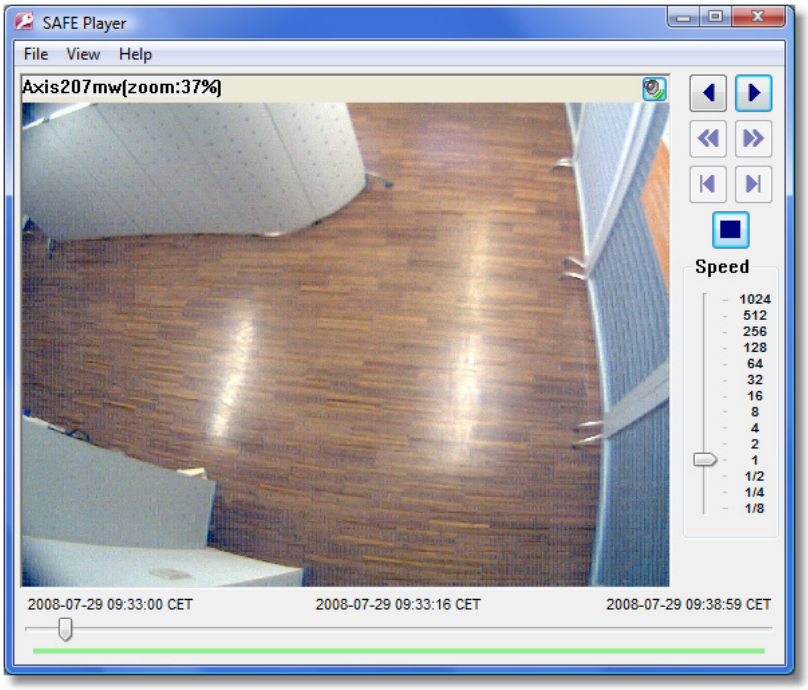
6.3.3 Exporting an archive recording in SAFE format

1. In the **Archive**, select a camera for the export.
2. In the **Player** view or in the **Calendar** view click the **Export** button to open the **Export** dialog.
3. Choose **SAFE (All images)** from **Export format**.
4. Enter the file for the video sequence to be exported.
   Mark the first checkbox if you want to overwrite a file of the same name that might exist.
5. Optionally you can create a **Multi-camera export** (synchronous video sequences) by clicking on the **Select camera** button . This opens the camera tree in which you can select multiple cameras by holding the **CTRL** key while clicking on the cameras.

6. Enter an **Export file label** which should describe the exported scenes.
7. Optionally you may enter an **Export file password**. This password is asked when the export file is executed (played).

Caution: Do not forget this password because otherwise you cannot replay this exported file.

8. When you click **OK**, a file dialog will be opened asking where on your client computer you to want to save the file. Once you select the location and confirm, a **File download progress dialog** will show the state of the export. You can cancel the export anytime by pushing **Cancel**.
9. The exported file is an executable for MS Windows XP/Vista/2000.
   Here is a screen dump of a running SAFE file:



Zooming in exported SAFE video sequences

You can zoom into parts of the camera view by drawing a rectangle and then clicking in the rectangle. You can drag a zoomed view with the mouse. Alternatively you can show the zoomed view in a separate window by selecting **View > Separate zoom window**. You can also use the mouse wheel to zoom in and out. See also *6.2.3 Zooming in a view port and in archive recordings* on page 49.

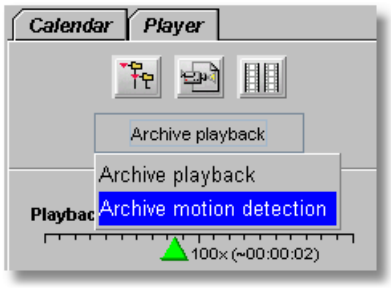
6.4 Motion detection in archive recordings

VisoGuard supports server-based motion detection not only for live camera streams but also in the archived recordings. Here you find information about how to execute motion detection on recordings.

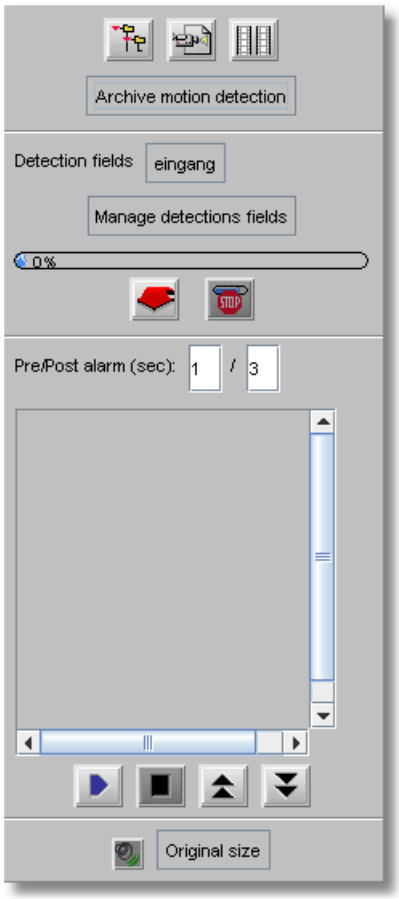
Please note: In this version, VisoGuard supports archive motion detection only for MJPEG recordings and not for recordings of other streaming formats (like MPEG-4 or H.264).

1. Go to the main window and choose the **Archive player** (if the Archive player is not available, then perhaps it is disabled in the client preferences; see *2.4 Client multi-window and multi-screen operation* on page 17).
2. In the **Calendar** view of the Player select the camera and the timeframe for the motion detection.
3. Push on the **Playback** button . This will load the images of the timeframe and replay the recorded images.

4. In the Upper left corner of the **Player** view select **Archive motion detection** from the **Control menu**:



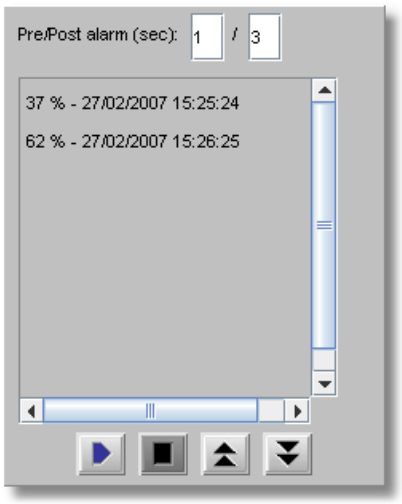
Now the motion detection pane is opened on the left side in the **Player** view:



5. From the **Detection field** pop-up menu choose the motion detection field definition you want to use for this motion detection. If you do not yet have a detection field defined or want to change an existing definition, then you can push the **Manage detection fields** button to jump to the Detection fields view in Administration. Please refer to *7.1.2 Basic configuration of server-based motion detection* on page 56 for details on how to setup detection fields.
Continuing here, we assume you have a correctly set up detection field definition.
6. To start the server-based motion detection Push the **Start** button .
You can see the progress of the motion detection at the progress bar. You can always stop a running motion detection by pushing the **Stop** button .

Caution: Since the motion detection actually runs on the VisoGuard server and can potentially use up a lot of CPU resources, please be careful selecting the detection fields and also the time period. Especially if you have selected a long time period in the Calendar the motion detection can take a lot of time. As mentioned above, you can always stop a running archive motion detection.

7. While the motion detection is running, the detected motions are displayed in the hit list sorted by the time in which the motion occurred. In our example, we have 2 hits:



8. You can replay the events by just selecting the event with the mouse. The playback time before and after the event can be defined by the **Pre/Post event (sec)** fields. You can change the values according to your needs. Please note that there must be archived pre- and post-event recordings available in order to be replayed.
9. You can step through the events by pushing the **Previous** and **Next** buttons.

7 Working with simple motion detection

Please note: Since release R1.12 VisoGuard offers powerful video analysis functions with iCAT. This chapter describes the simple motion detection features that were present before R1.12 and that are now a part of the iCAT toolbox. Simple motion detection is based on a detection of changed pixels between video frames while iCAT offers intelligent object detection and tracking. For more details on iCAT refer to *14 Video analytics with iCAT* on page 96.

VisoGuard offers two mechanisms for simple motion detection:

- **VisoGuard's own server-based motion detection**: The images are analyzed by the VisoGuard server. The advantage of this method is that it works with any camera, even old cameras. The disadvantage might be that if there are many cameras that transfer their images to the server for analysis, the bandwidth of the network could be burdened and also the server could be overloaded.
- **In-camera motion detection**: The images are analyzed in the camera and only when detection occurs, an event and image data are sent to the VisoGuard server that then stores the event and the images in its archive. The advantage of this method is that the network and the server are not burdened. The disadvantage is that it works only with special cameras, that offer this feature and that the motion detection settings have to be programmed in the camera directly.

7.1 VisoGuard's own server-based motion detection

The simple motion detection feature of VisoGuard can recognize motion by detecting pixel changes between video frames. Such a detection can then trigger the following predefined actions:

- Entry of events in an Event list optionally accompanied by an acoustic signal
- Changes in recording behavior (e.g. higher recording rate) if that has been programmed (see *6 Working with archive recordings* on page 43).

Here you find the steps how to configure the parameters for simple motion detection.

7.1.1 Preparation

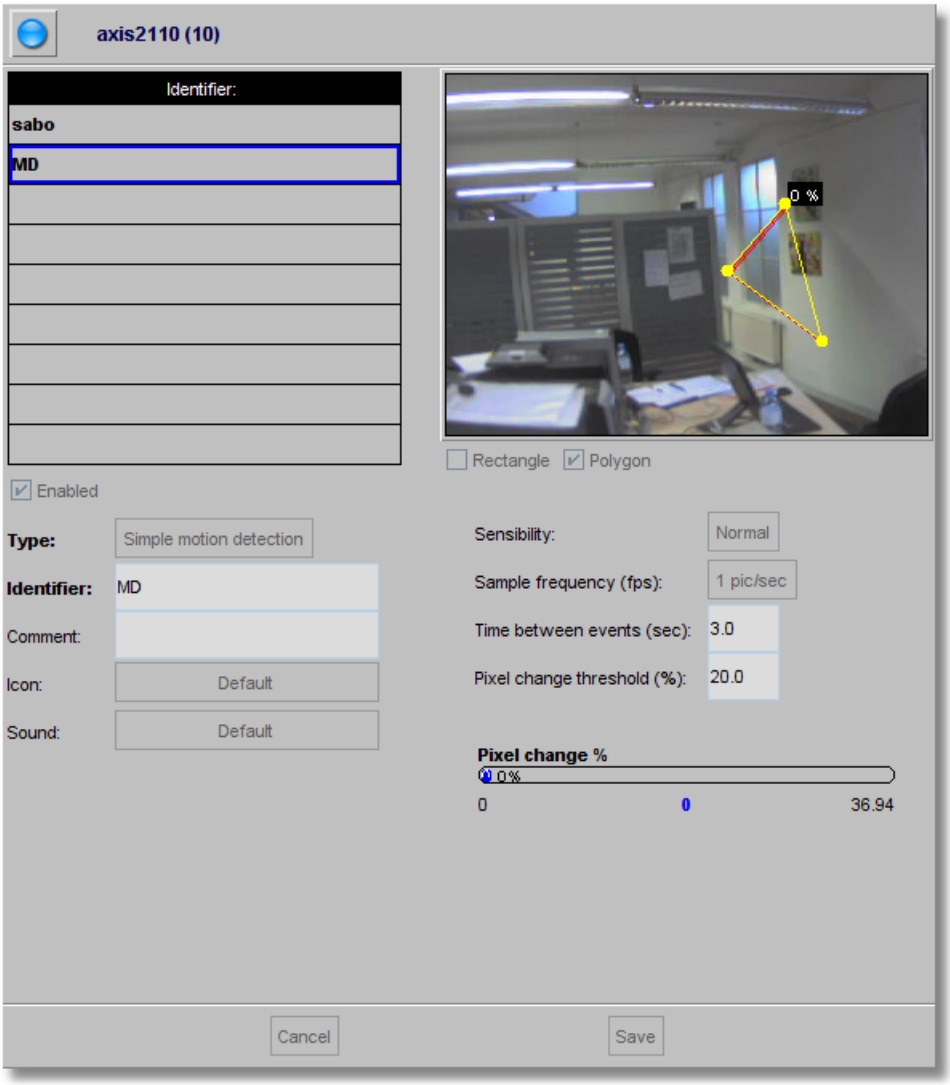
Before you begin to configure a motion detection definition, be sure that you have the necessary authorization to make settings. If you are not sure, please ask your VisoGuard administrator.

Please note: Motion detection for PTZ cameras is problematic since normal movement of the camera will trigger a motion detection event.

7.1.2 Basic configuration of server-based motion detection

If you are not already running the VisoGuard client application, open your Internet Explorer and log in to your VisoGuard server and your VisoGuard system.

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.



2. In the camera tree at the left, select the camera for which you want to create a motion detection definition.
3. In the menu choose **Add new definition**.
4. From the **Type** menu chose **Simple motion detection**.
5. Select whether you want to create a **Rectangle** or a **Polygon**.
6. Use the mouse to draw a detection field in the preview area.
7. Mark the **Enabled** checkbox, otherwise the detection field is inactive and no detection can occur. Actually, a detection field must also be assigned to an active motion detection schedule (see below).
8. Assign a name for the field in the **Identifier** text box, e.g. “Movement”.
9. Optionally, you can enter a **Comment** (Please note .
10. Usually the **Sensitivity** should be left at **Normal**. It defines how sensitive (or tolerant) the detection algorithm is when detecting the change of pixels. Modify the setting only when you want the algorithm to be more or less sensitive.
11. In the **Sample frequency (fps)** field you can specify how often the image is to be checked for changes.
12. In the **Time between events (sec)** field you can enter the minimum time that must elapse before a following event is triggered. This helps to filter out repetitive events.
    Minimum time (sec) = 3 means that, after one motion detection event has been triggered, at least 3 seconds must pass before another Motion Detection event can be generated.

13. In the **Pixel change threshold (%)** field you can define how many pixels in % must change so that a detection event is triggered.
    Pixel change (%) = 20 means that 20% of the pixels relative to the previous frame (detection cycle) must change for a detection to be triggered.
14. Optionally you can define a specific event icon and sound for this definition: Click on the **Icon** button to assign a symbol. This icon is displayed in the **Event list** to notify an operator when an event related to this definition occurs.

    Click on the **Sound** button to assign a specific sound to the definition. This sound is played when a user notification event related to the definition occurs.

15. After you have entered all parameters for your definition, save it by clicking on the **Save** button.
16. If you have not yet scheduled a detection-based recording for this camera, you will be prompted for whether you want to edit the scheduling now.

    Click on the **Yes** button if you want to configure the scheduling now. Please refer to section *7.1.3 Scheduling motion detection* on page 58.

    Click **No** if you want to do that later.

Please note:
If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually.
If a definition is not assigned to an active schedule then it will not be activated (no archive recordings will be made and no events will be generated) although it has the **Active** option set.

7.1.3 Scheduling motion detection

The scheduling for simple motion detection is the same as for other iCAT definitions. Please refer to *14.3.9 Scheduling iCAT operation and recording* on page 110.

7.1.4 Controlling PTZ cameras with server-based motion detection events

It is possible to assign a sequence of PTZ positioning actions to each motion detection (MD) field definition. Once the MD field gets active, the associated PTZ action is executed. PTZ actions can be assigned to an MD field by appending the following sequence to the MD **Identifier**:

ptz:<CID>:<PresetName>:<WaitTime>:<PresetName>:<WaitTime>...

where:

<CID> is the ID of a PTZ camera (the ID is shown in **CameraAdmin Properties** dialog next to the camera name). If <CID> is 0, then the MD field's camera is controlled (MD and PTZ camera are the same).

<PresetName> is the name of a preset position (as entered in the PTZ definitions).

<WaitTime> is the pause time in seconds starting from the time when the camera receives the positioning event.

There can be any number of "**<PresetName>:<WaitTime>**" pairs added.

Further MD-triggered PTZ actions are blocked as long as a sequence is running. However, control of PTZ camera can be taken manually, then the automatic MD-triggered PTZ control is suspended until the manual PTZ control is released.

For information on how to setup PTZ preset positions refer to *9 Working with PTZ cameras* on page 66.

Example:

Door ptz:4:Door:10:HomePos:3

will on an MD event with the **Identifier** “Door” move the PTZ camera with ID 4 to the preset position “Door”, wait 10 seconds and move the camera to the preset “HomePos” and wait another 3 seconds. The overall positioning time therefore is app. 13 seconds. From then on the PTZ camera is open to receive further MD-triggered PTZ positioning commands.

7.2 Motion detection in archive recordings

VisoGuard supports server-based motion detection not only in live streams but also in archived recordings. Please refer to *6.4 Motion detection in archive recordings* on page 53.

7.3 In-camera motion detection

Several IP cameras and video servers support in-camera motion detection and upload (push) of event-triggered images via FTP or HTTP to a video management system like VisoGuard. VisoGuard implements a general mechanism to handle this feature.

This section describes how VisoGuard supports in-camera motion detection and also how to configure it in VisoGuard.

Please note: Since the camera carries out the detection, the actual configuration and programming must be done directly in the camera via the setup interface (e.g. parameters like detection settings, image quality, speed, etc.). This can usually be done by connecting with a web browser to the camera (by entering its IP address). Please refer to the most actual document *Thecus VisoGuard 4.0 Supported Video Sources* and the camera’s user manual for further details.

7.3.1 How VisoGuard supports in-camera motion detection

In the camera you define the various settings for the motion detection algorithm and for the transmission of event images to the VisoGuard server, which is done via FTP or HTTP ("push upload" by the camera). Most cameras also support the transmission of pre- and post-event images. The configuration of for these pre- and post-event images must also be done in the camera.

VisoGuard is capable of doing these things in connection with in-camera motion detection:

- **Receive in-camera motion detection events** from the camera and store these events in the standard VisoGuard Event database (these events can also be displayed in the Task bar).
- **Receive pre- and/or post-event images** from the camera (pushed by the camera) and record these images in the standard VisoGuard camera archive.
- Optionally, with receiving an in-camera detection event, **start a server-based post-event recording** of images and merging this recording with the in-camera event images pushed by the camera. This server-based recording can have a much higher frame rate than the pictures pushed by the camera. This allows a much better documentation of in-camera events.

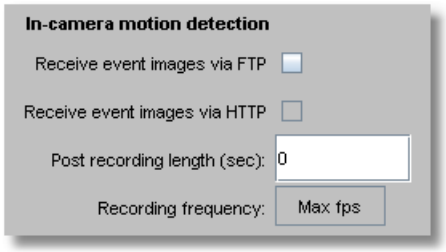
7.3.2 Setting up in-camera motion detection

To configure VisoGuard for in-camera motion detection follow these steps:

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.

   Assuming that you have already defined the basic properties of the camera in VisoGuard, select the camera in the camera tree.

2. On the **Properties** dialog push the **Next** button at the bottom of the dialog until you reach the **Defaults settings** dialog. Here you focus on the **In-camera motion detection** settings:



3. In the menu choose **Modify selected camera or group**.
4. Mark either **Receive event images via FTP or …via HTTP** depending on what your camera supports. This tells VisoGuard to receive in-camera events and images from the camera.
   If you already have a defined an active server motion detection schedule for the camera, you will get a dialog that tells you that having both, server and in-camera motion detection at the same time is not possible. To continue you have to first disable the server-based motion detection schedules in the **Scheduling** dialog and then you can continue here.
5. Optionally you can set the **Post recording length (sec)** that defines whether and for how long the VisoGuard server should record camera images in addition to receiving and storing the event pictures pushed by the camera. As mentioned above, you could want to do that to record the post-event images with a high frame rate. In such a case, set the **Frame rate** according to your needs.
6. Now you also have to tell VisoGuard, for how long it should keep the recorded event-images (both, the ones pushed by the camera and the ones, additionally recorded by the server).
   Push **Previous** button at the bottom of the dialog until you reach the **Scheduling** dialog.
7. Below the **Time intervals** list push the **Add** button and then choose **Camera MD (FTP/HTTP)** from the newly created **Change** pop-up menu.
8. In the field **Requested recording period (days/hours)** enter the values that fits your needs. Optionally you can also mark the **Priority over other cameras (if storage space is short)** checkbox. For further details about these recording parameters please refer to sections *6.1.1 Programming continuous timed recordings* on page 43 and *6.1.3 Operation of the VisoGuard dynamic storage management* on page 45.
9. Push the **Save** button to store your changes.
10. Now you have to configure your camera for pushing the in-camera events and images to the VisoGuard server. Since the steps for doing that are very camera-specific, you must consult the document *Thecus VisoGuard 4.0 Supported Video Sources*. To program the camera's detection algorithm please consults its user manual.

Note: After setting up the camera, do not forget to check and set the date and time of the camera to reflect your current time.

8 Handling events

VisoGuard can record and display events of various types. They can be camera-related events like video analytics events, archive access by a user, or camera failures, but also system-related events like user logon and logoff.

Events are displayed in Event lists of the client and are stored in the central event database of the VisoGuard server were they can also be queried. The can have several properties that depend on the type of the event.

Event priorities

All events also have an event priority that defines the relative importance of events. The default event priority is 100. Informational events have a lower priority of 50, system and camera malfunction events have a higher priority of 300. For events generated by video analytics triggers, you can specify individual event priorities. Event lists can also be sorted according to priority.

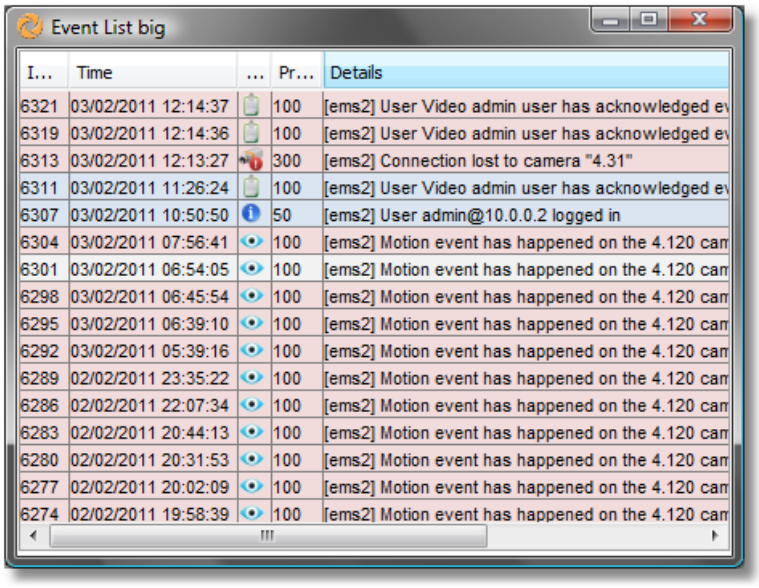
User privileges for accessing and handling events

In the **User admin** under the **System administration** menu you can define for each user some basic event handling privileges. For example whether user you can access events at all or what kinds of system events are displayed at the users event list (see *4.2 Setting general user privileges* on page 30).

The number of events stored in the database can be defined in the server parameters (see *10.2 Setting VisoGuard server parameters* on page 75).

8.1 Event list and event details

The most actual events are displayed in the **Event list**:


Event List big
I...
Time
...
Pr...
Details
6321 03/02/2011 12:14:37 100 [ems2] User Video admin user has acknowledged ev
6319 03/02/2011 12:14:36 100 [ems2] User Video admin user has acknowledged ev
6313 03/02/2011 12:13:27 300 [ems2] Connection lost to camera "4.31"
6311 03/02/2011 11:26:24 100 [ems2] User Video admin user has acknowledged ev
6307 03/02/2011 10:50:50 50 [ems2] User admin@10.0.0.2 logged in
6304 03/02/2011 07:56:41 100 [ems2] Motion event has happened on the 4.120 cam
6301 03/02/2011 06:54:05 100 [ems2] Motion event has happened on the 4.120 cam
6298 03/02/2011 06:45:54 100 [ems2] Motion event has happened on the 4.120 cam
6295 03/02/2011 06:39:10 100 [ems2] Motion event has happened on the 4.120 cam
6292 03/02/2011 05:39:16 100 [ems2] Motion event has happened on the 4.120 cam
6289 02/02/2011 23:35:22 100 [ems2] Motion event has happened on the 4.120 cam
6286 02/02/2011 22:07:34 100 [ems2] Motion event has happened on the 4.120 cam
6283 02/02/2011 20:44:13 100 [ems2] Motion event has happened on the 4.120 cam
6280 02/02/2011 20:31:53 100 [ems2] Motion event has happened on the 4.120 cam
6277 02/02/2011 20:02:09 100 [ems2] Motion event has happened on the 4.120 cam
6274 02/02/2011 19:58:39 100 [ems2] Motion event has happened on the 4.120 cam

Each client can have multiple event lists, for example, one that is sorted chronologically and another one that is sorted according to event priorities. In the client preferences (accessible via **Client preferences...** in the **Observer** menu) you can define for each event list what columns are to be displayed and whether acknowledged events should stay in the list or should disappear automatically (which is the default behavior).

The position of the event lists inside client windows and further layout options can be defined as described in *2.4 Client multi-window and multi-screen operation* on page 17

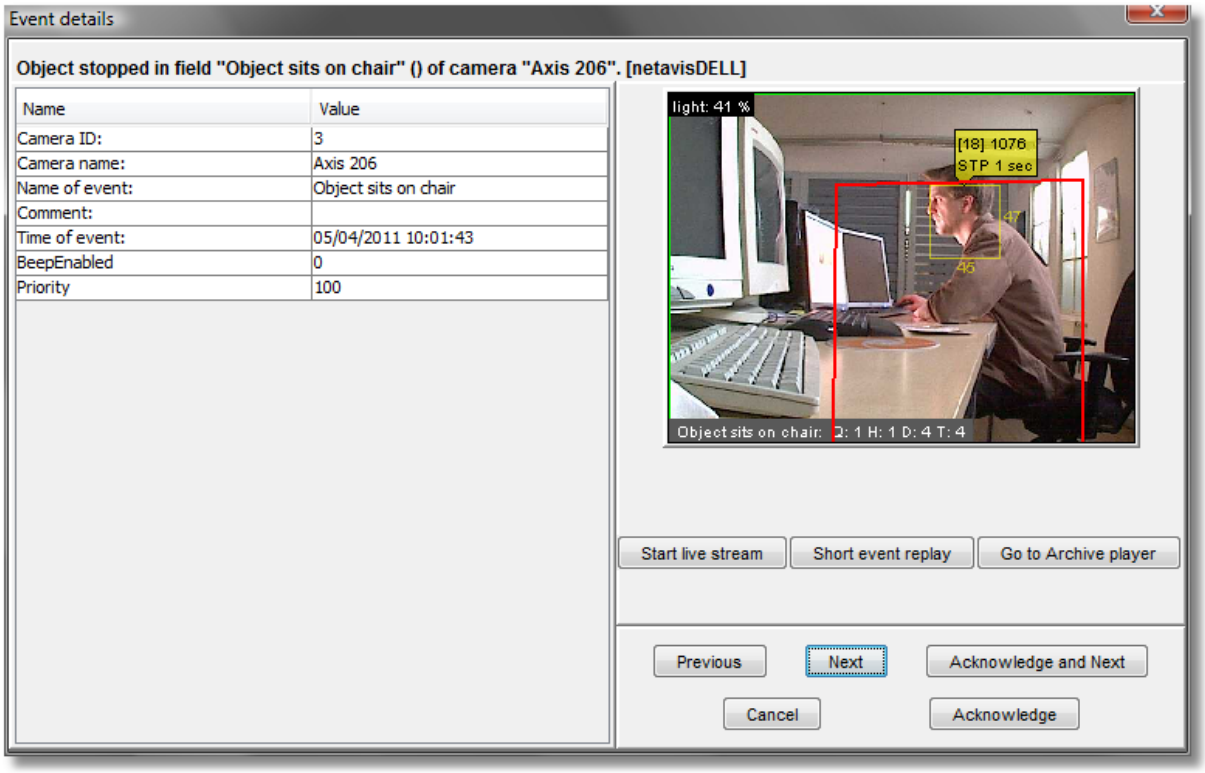
You can sort the event list according to column values by just clicking on the column title. Little arrows after the title indicate the sorting order (ascending or descending). Clicking a column title again will change the sorting order. For example, you can sort the list according to event priority by clicking on the **Priority** column heading.

In an event list columns can be rearranged by clicking on a column title and dragging it with the mouse to the new location.

Unseen events have a light red background color. As soon as an event has been opened in the **Event details** dialog its background color changes to light grey. When an event is acknowledged, it usually disappears from the event list. However, in the client preferences you can define whether acknowledged events should be displayed in the event list. If so, they appear with a white background color.

8.1.1 Event details

Double clicking on an event in the event list opens the **Event details** dialog.



If you want to examine details of an event, simply click on its symbol. An **Event** viewer opens.

The first line contains the event text. Further details of the event are listed at the left side of the dialog. The exact contents of the event details depends on the event type, but you will find the exact time when the event occurred and if it is a camera-related then also the camera ID and name are shown.

When you move the mouse over the camera preview area you will also see the video analytics object markers and annotations related to the event trigger (as seen in the screen shot above).

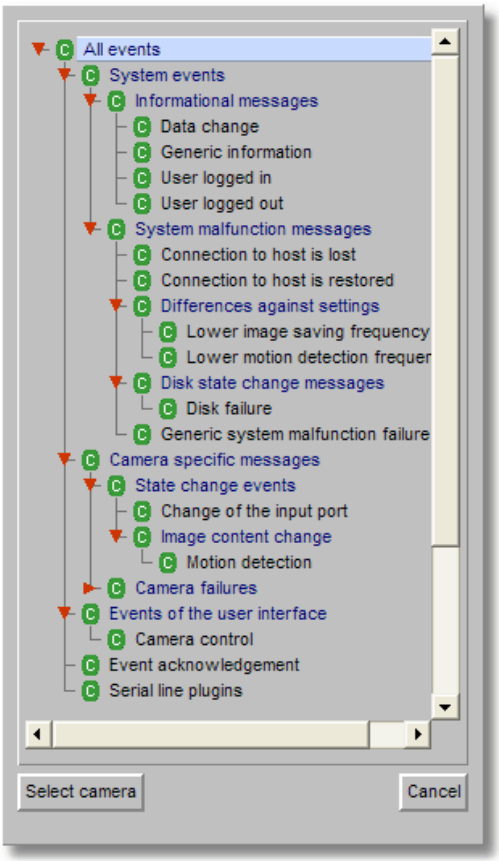
Here is what you can do in the dialog by pushing various buttons:

- **Start live stream**: starts live monitoring of the camera that triggered the event .
- **Short event replay**: starts a playback of the event recording that triggered the event (a replay is only available if the camera has been configured: record on the event).
- **Go to Archive player**: opens the Archive player and starts a playback of the event recording.

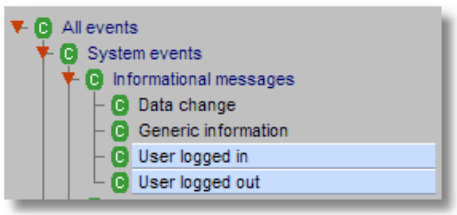
- **Previous**: loads the previous event.
- **Next**: loads the next event.
- **Acknowledge and next**: acknowledges the event and loads the next event.
- **Acknowledge**: acknowledges the event and close the dialog.
- **Cancel**: closes the dialog.

8.2 Searching in the event database

1. When you choose **Event search...** from the **Events** menu the **Event search** dialog appears.
2. Select the **Time filter** according to your needs.
3. Push **Search** to display the results.
4. You can further constrain the search by setting values for **Event type**, **Name of camera**, **Name of user**, or **Event ID (from- to)**. For some values an appropriate dialog will open, e.g. the Event selection dialog:



It each of the dialogs it is possible to make multiple selections. For example to search for the event types **User logged in** and **User logged out**, hold down the **CTRL** key and select these event types with left mouse clicks:



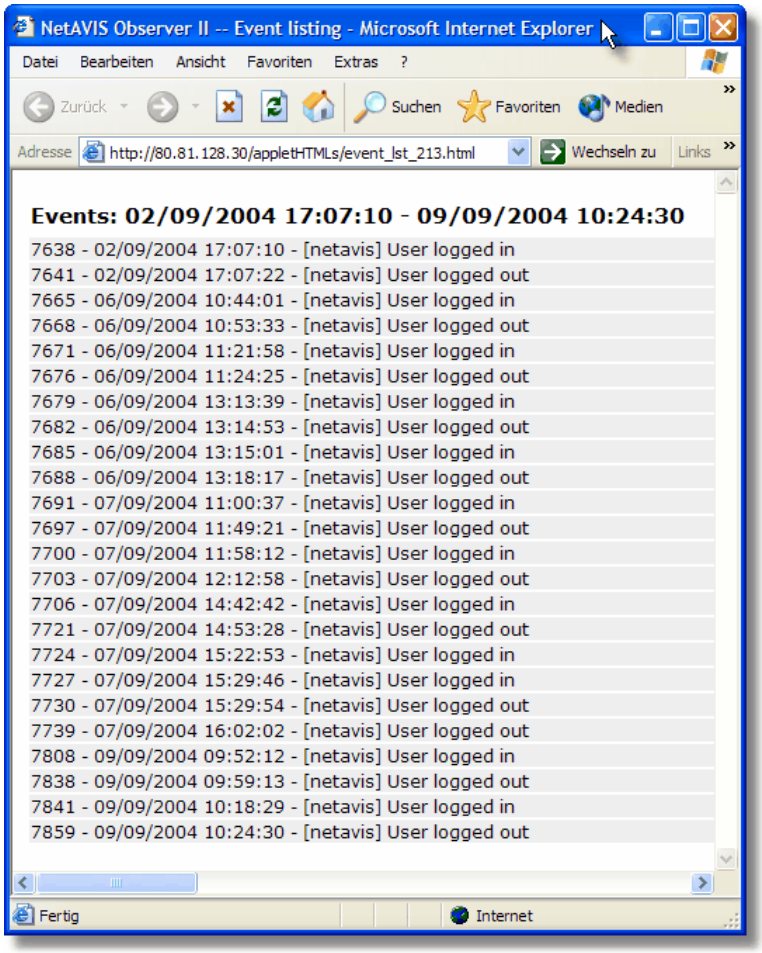
You can also search for events which are **acknowledged** or **not acknowledged** by selecting the appropriate check box.

5. After setting different search criteria push the **Search** button again to display the results.

   By clicking the **Next** button you can step forward in the result list and with **Previous** button you can step back.

8.2.1 Saving results in an HTML file

1. You can also save the search results directly to an HTML file by selecting the **Save results in HTML document** checkbox.
2. Set the **Number of records** pop-up menu to **All**.
3. After clicking the **Search** button a file dialog will open asking for a file name. Enter a file name and choose a location and click **Save**.
   Now the file is created. You can open the file in a normal web browser:

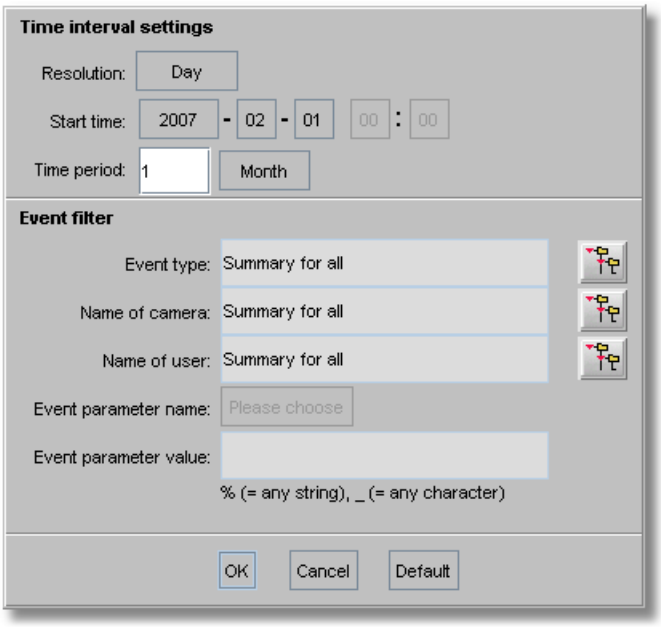

NetAVIS Observer II -- Event listing - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse http://80.81.128.30/appletHTMLs/event_lst_213.html
Wechseln zu Links
Events: 02/09/2004 17:07:10 - 09/09/2004 10:24:30
7638 - 02/09/2004 17:07:10 - [netavis] User logged in
7641 - 02/09/2004 17:07:22 - [netavis] User logged out
7665 - 06/09/2004 10:44:01 - [netavis] User logged in
7668 - 06/09/2004 10:53:33 - [netavis] User logged out
7671 - 06/09/2004 11:21:58 - [netavis] User logged in
7676 - 06/09/2004 11:24:25 - [netavis] User logged out
7679 - 06/09/2004 13:13:39 - [netavis] User logged in
7682 - 06/09/2004 13:14:53 - [netavis] User logged out
7685 - 06/09/2004 13:15:01 - [netavis] User logged in
7688 - 06/09/2004 13:18:17 - [netavis] User logged out
7691 - 07/09/2004 11:00:37 - [netavis] User logged in
7697 - 07/09/2004 11:49:21 - [netavis] User logged out
7700 - 07/09/2004 11:58:12 - [netavis] User logged in
7703 - 07/09/2004 12:12:58 - [netavis] User logged out
7706 - 07/09/2004 14:42:42 - [netavis] User logged in
7721 - 07/09/2004 14:53:28 - [netavis] User logged out
7724 - 07/09/2004 15:22:53 - [netavis] User logged in
7727 - 07/09/2004 15:29:46 - [netavis] User logged in
7730 - 07/09/2004 15:29:54 - [netavis] User logged out
7739 - 07/09/2004 16:02:02 - [netavis] User logged out
7808 - 09/09/2004 09:52:12 - [netavis] User logged in
7838 - 09/09/2004 09:59:13 - [netavis] User logged out
7841 - 09/09/2004 10:18:29 - [netavis] User logged in
7859 - 09/09/2004 10:24:30 - [netavis] User logged out
Fertig
Internet

8.3 Generating an event statistics report

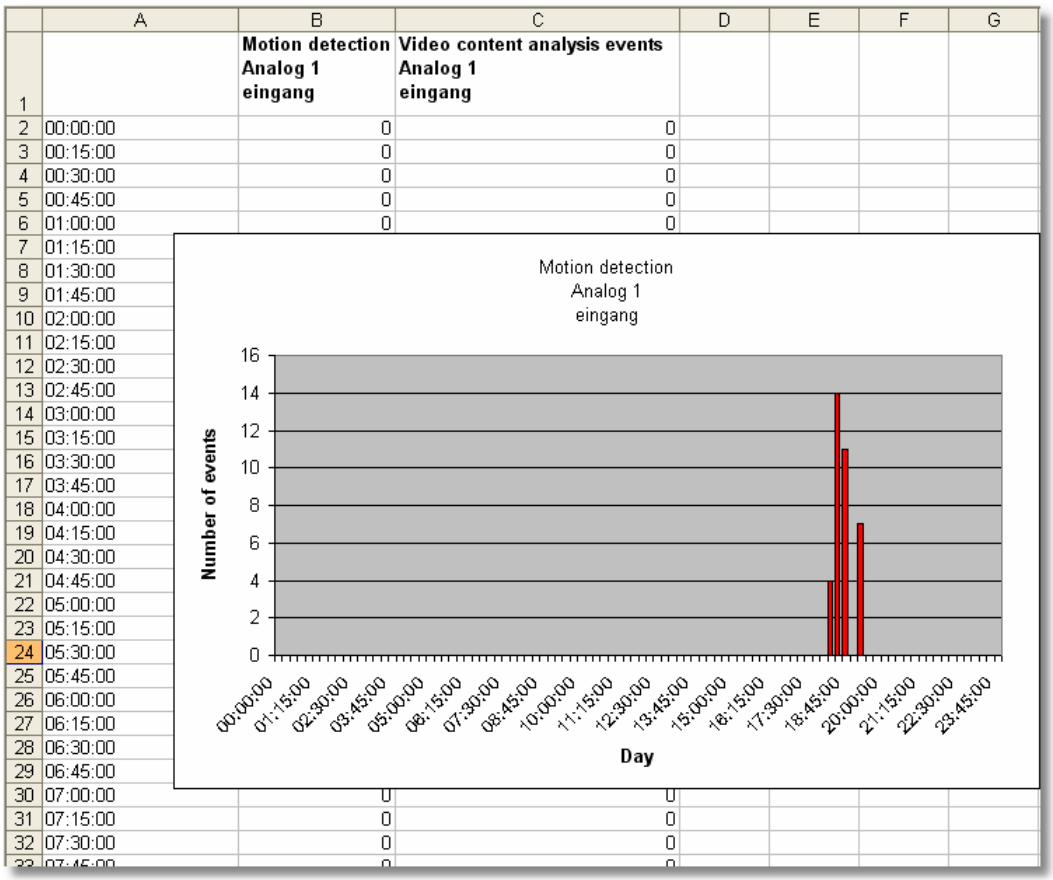
VisoGuard allows you to create an event statistics report in MS Excel XLS format.

To create a statistics report file, follow these steps:

1. Choose **Event statistics export...** from the **Events** menu.This brings up the **Event statistics export** dialog:



2. Select for which **Start time**, **Time period** and time **Resolution** you want to create the report. Also you can filter according to **Even type**, **Camera** and **User** (multiple selection by holding down the **CTRL** key while clicking is supported for all filters). If you do not select any values for Event filter, then a summary statistic report will be created.
3. Push **OK** to start creating the report file. You will be prompted for a file name where the report should be stored.
4. Open the created file in MS Excel. With the data, you can also create graphics like the following one (motion detection statistics for one day):



9 Working with PTZ cameras

VisoGuard features the control of PTZ cameras (pan/tilt/zoom).

Note: To configure and work with PTZ cameras, you need the corresponding user privileges and camera access rights (see *4.2 Setting general user privileges* on page 30 and *4.3 Setting camera access rights* on page 31). If you find that you do not have the authorizations you need, please contact your VisoGuard administrator.

9.1 Setting up a PTZ camera

Setting up a PTZ camera is the same procedure as setting up a camera without PTZ functionality (*3 Setting up cameras* on page 20).

The user must possess the user-specific camera authorizations (see *4.3 Setting camera access rights* on page 31) to permit PTZ access.

9.2 Defining fixed PTZ positions

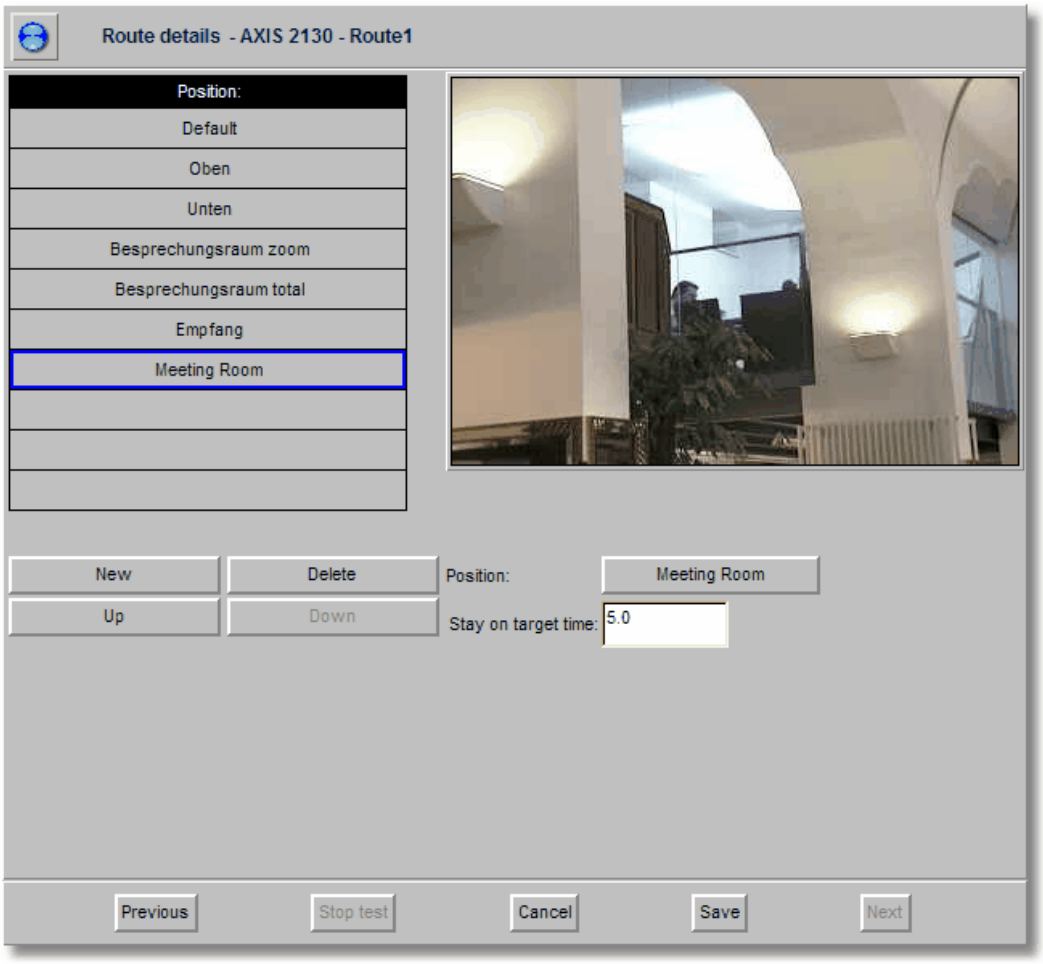
1. Choose **PTZ** from the **System administration** menu. This opens the **PTZ** dialog.
2. From the camera tree, select the PTZ camera whose PTZ positions you want to program.
3. In the menu select **Add new definition**.
4. In the **Name** field enter a designation for the position and then use the **PTZ control elements** to move to the desired position (detailed explanation of control elements in Section *9.4 Controlling PTZ cameras* on page 67):
5. Click on **Save** to save your configuration. Then you can repeat steps 3 to 5 to define additional PTZ positions.
6. From the **Online Monitor** you can select these predefined positions (see below).
7. Double-clicking on one of the predefined positions lets you position the camera. Proceed similarly in order to change positions.

9.3 Defining PTZ routes

In addition to individual PTZ positions, you can also define position routes that can be followed on command. A position route consists of a list of PTZ positions that are automatically, sequentially followed and a duration per position.

Define a PTZ route as follows:

1. Choose **PTZ** from the **System administration** menu. This opens the **PTZ** dialog.
2. From the camera tree, select the PTZ camera whose PTZ route you want to program.
3. If you have not already defined PTZ positions that now appear in the list, or you can create new positions now. See the previous section for defining new positions.
4. Click on the **Next** button at the bottom right. This takes you to the **Routes** dialog, whose layout resembles the **Positions** dialog above.
5. In the menu select **Add new definition**.
6. In the **Name** field enter a designation for the route. Optionally you can enter a description.
7. Click on **Next** to move to the **Route details** dialog:



8. Click the **New** button to create a new entry in the **Position** list of the route and select a position from the list of predefined positions via the **Position** popup menu.
9. In the **Time at position** field, enter the duration in seconds that the camera is to spend at the position. Note that this time includes the positioning time of the camera.
10. Repeat Steps 8 and 9 for each entry in the position list.
11. You can change the sequence within the position list by selecting a position and then clicking the **Up** or **Down** button. You can remove an entry from the **Positions** list by selecting it and then pressing the **Delete** button.
12. Click the **Save** button to save your route or **Cancel** to discard changes.

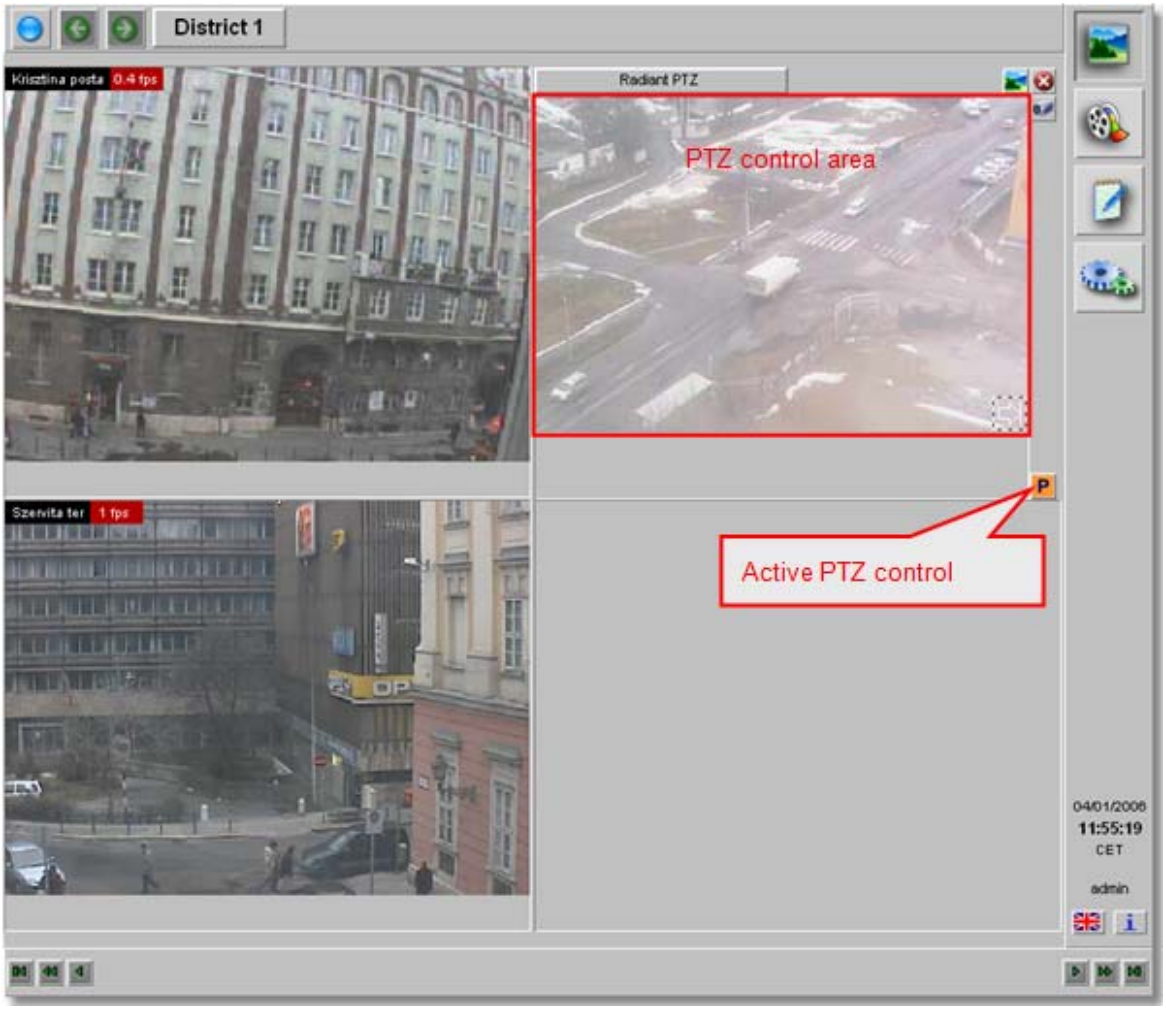
You can select the saved route in the Online Monitor via the **PTZ** menu of the view port control menu of the PTZ camera. Proceed similarly to modify a route.

9.4 Controlling PTZ cameras

9.4.1 Controlling PTZ cameras in the Online monitor

Control PTZ cameras as follows:

1. Select the **Online monitor**.
2. Switch to a view that contains a PTZ camera (how to create views and assign cameras is covered in section *5 Using the Online monitor* on page 34).
3. In the view port of the PTZ camera push the PTZ start button or choose **PTZ->Activate PTZ** from the view port control menu. The icon P of the view port indicates that you have PTZ control over the camera.

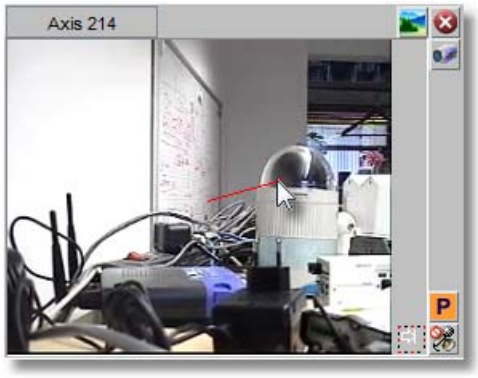


Note: For each user a PTZ priority and allocation timeouts can be defined (see *4.1 Creating a new user account* on page 29). If another user with equal or higher priority has already assumed PTZ control over the camera, you will be denied control and notified in a window. Then you need to wait until this user surrenders control or reaches his timeout.
A user with a higher PTZ priority can take away PTZ control from a user with lower PTZ priority.

Direct PTZ control inside a view port

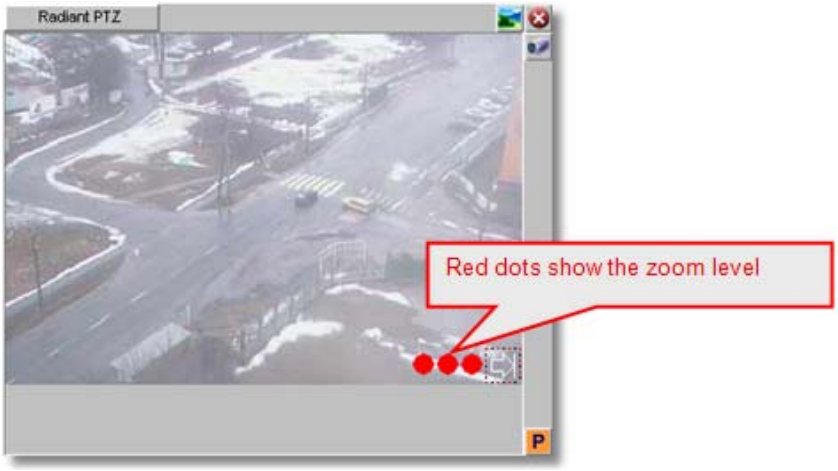
You have several options for directly controlling PTZ cams: The various modes can be selected via **PTZ->PTZ control mode** in the view port control menu. The default setting is **Continuous** mode and **Center on click**. As an alternate mode also an operation via a **Crosshair** is available.

Continuous mode (available for joystick and mouse operation): Click the mouse in the view port and drag it in the direction where you want the PTZ cam to move. A red line indicates how fast the movement is. When you release the mouse, the movement will stop.



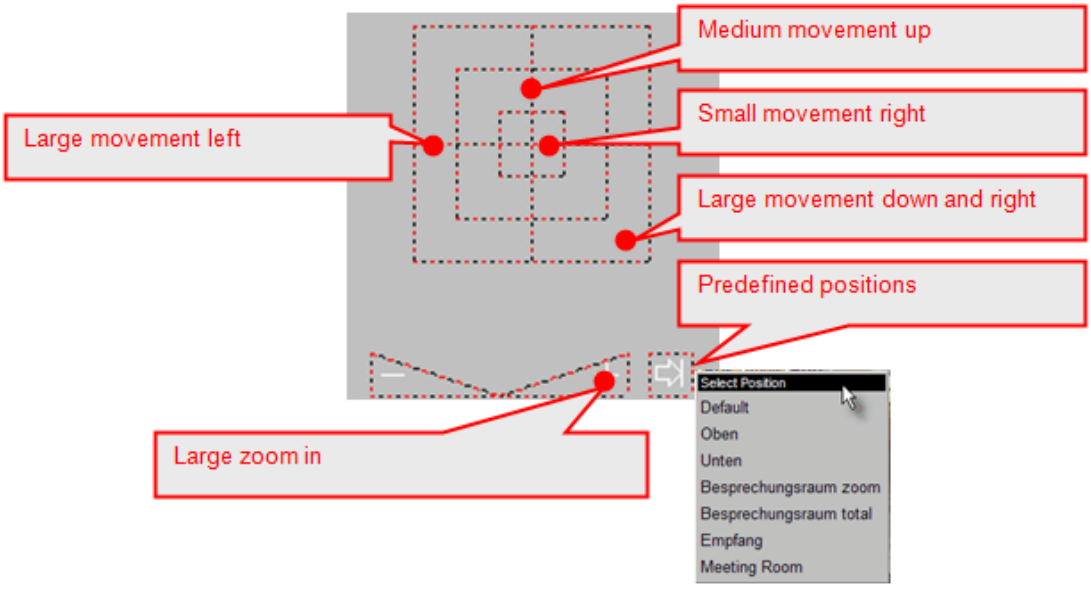
Center on Click: A single mouse click somewhere in the view port commands the camera to center on the mouse click location.

Zooming: Zooming is available via the mouse wheel: zoom-in (forward scroll) and zoom-out (backward scroll). The amount of the zoom will be indicated by 3 red dots after the mouse is released:



Please note: When PTZ control is enabled, any mouse actions are taken for PTZ control. In order to control the client-based view port zooming (see *6.2.3 Zooming in a view port and in archive recordings* on page 49), hold down the **CTRL** key while using the mouse.

Crosshair: When this mode is enabled, a crosshair is shown in the view port



Controlling PTZ cameras with a joystick:

The locally installed version of VisoGuard is able to handle USB joysticks as input device from Java VM 1.4 and newer (for information on how to install the application version locally please refer to *2.3 Working with the installed VisoGuard client* on page 14.

The joystick can be used for panning, tilting the camera, while its buttons for zoom-in and zoom-out operations (which button is used for which operation is assigned during calibration). The joystick must be calibrated before use (found in the System Information menu, beside the language change menu). To "assign" the joystick input focus to a camera, click into the frame while holding the SHIFT and CTRL buttons. This is visible via an in-picture icon drawn when the assignment is successfully done.

Jump to a predefined PTZ position and follow PTZ routes

1. To spot a camera to a predefined PTZ position, click on the right arrow at the lower right corner of the view port and select a position from the list (see *9.2 Defining fixed PTZ positions* on page 66).
2. To automatically follow a predefined PTZ route choose it from **PTZ->Select PTZ route** in the view port control menu of the PTZ camera.
3. In the view port control menu of the PTZ camera, click **PTZ->Select PTZ route->Stop route** to stop control of the PTZ camera.

Stop PTZ control

You can stop PTZ control by pushing the button or deselect **PTZ->Activate PTZ** control in the view port control menu.

Note: Please do not forget to stop PTZ control; otherwise other users cannot assume control. When you end the VisoGuard client, all PTZ control is automatically released.
For further details on user-specific PTZ priorities and timeouts please refer to *4.1 Creating a new user account* on page 29.

9.4.2 Controlling PTZ cameras with motion detection events

It is possible to automatically control PTZ cameras with motion detection events. Please refer to *7.1.4 Controlling PTZ cameras with server-based motion detection events* on page 58.

9.4.3 Scheduling PTZ routes

It is possible to schedule time intervals for PTZ camera to follow predefined routes.

Note: Before you can schedule a route you first must define the route (please refer to *9.3 Defining PTZ routes* on page 66).

To schedule a PTZ route, follow these steps:

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.
2. Select a PTZ camera.
3. Press the **Next** button to go to the **Scheduling** dialog.
4. In the menu select **Modify selected camera or group**.
5. Click the **Add** button to add a programming slot to the **Time Intervals field**.
6. Click the **Change** button (now enabled) for a popup menu; select **PTZ route**.
   This will show the PTZ scheduling settings (see above).
7. Set the **time settings** according to your needs.

8. Select the route from the **Route Name** pop-up menu (in the example above we selected Route 1).
9. Click on **Save** to store the scheduling settings.

Note: You can add several PTZ route schedules for a single camera. This means that you can follow different routes at different times.

10 Administrating VisoGuard servers

This chapter describes how to get status information about an VisoGuard server and how to set server parameters. Further information about administrating servers you find in the document *Thecus VisoGuard 4.0 Server Installation and Administration*.

10.1 Server system information and restarting

VisoGuard offers 2 sets of status information of the running servers in a network.

- The server load display in the main client window
- The System information dialog in the Admin area

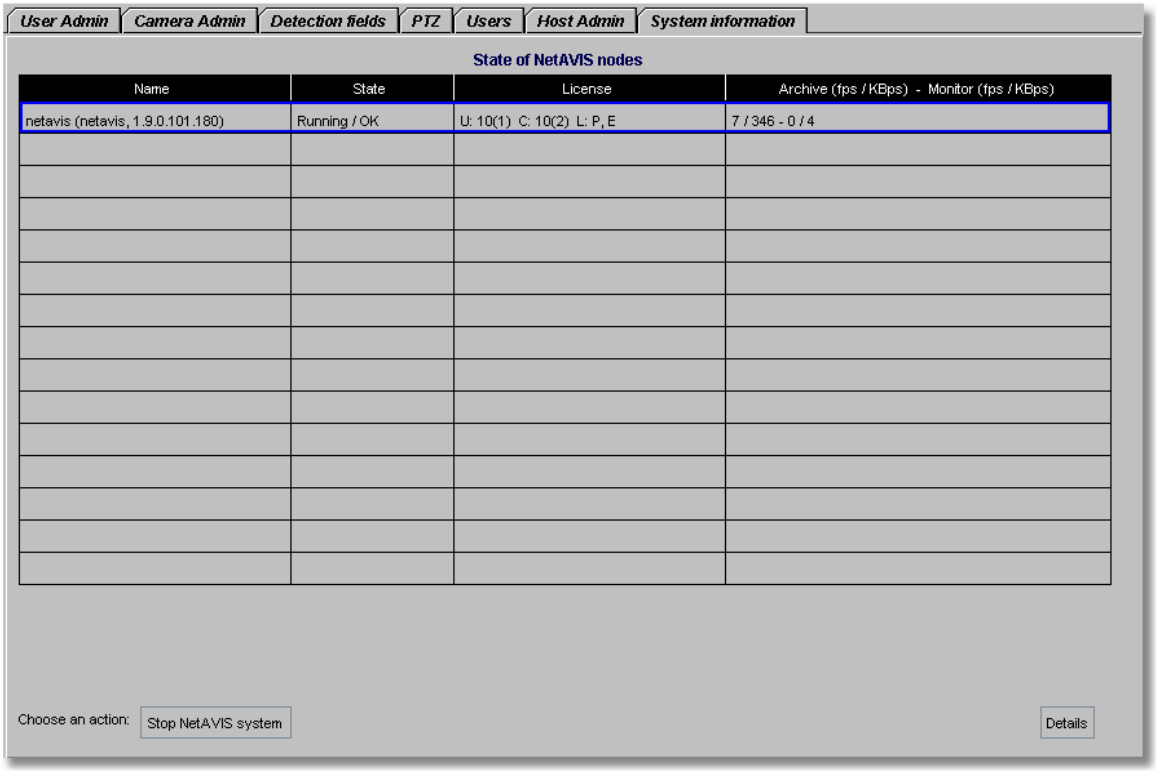
10.1.1 Server load display

The server load display is located in the status bar of the main client window and shows the following information:

CPU: xx %	Server CPU load in percent. This display is updated every 5 seconds.
IDB: xx % xx KB/s	Load of Image database (IDB) engine: This parameter shows how busy the server is with saving video data on storage. The actual video data storage rate is displayed below the percent value in Megabytes/sec or Kilobytes/sec. The IDB display does not appear if the server does not record. Note that the IDB load also increases when the server removes video data when the storage is full or recording time limits are reached. IDB details are updated once a minute.
OVR: xx %	Overloaded state of the IDB engine: The IDB engine is overloaded if the server receives more video data from the cameras than it can record (save on storage). In this case the server will drop frames. OVR shows the percent of dropped frames. If the label OVR does not appear then the server can save every incoming frame.
SWP: xx MB	Swapping: This display appears if the server starts heavy swapping, which means that the amount of main memory of the server is insufficient. If this is situation persists, the server must be extended with additional RAM.

10.1.2 System information dialog in the Admin area

1. Choose **System information** from the **System administration** menu. This opens the **System information** dialog.



The table shows the connected servers and their state:

Name shows the name of the server and the VisoGuard version running.

State shows whether the server is running and if there is a failure (the server in the screenshot above is running OK).

License shows the license of the VisoGuard server:

- **U**: shows the number of total and in parentheses the number of used-up user licenses. If the number contains an “R” then it is a floating license from a remote licensing server.
- **C**: shows the number of total and in parentheses the number of used-up camera licenses. If the number contains an “R” then it is a floating license from a remote licensing server. If the number of cameras exceeds the license limit, then in parentheses first the number of disabled cameras is shown and then, after a slash, the number of allowed licensed cameras.
- **L**: shows the license type and the licensed product edition and modules:

  License type:
  P = permanent license
  D = demo license

  Licensed product edition:
  B = VisoGuard Basic edition
  C = VisoGuard Core edition
  E = VisoGuard Enterprise edition
  X = VisoGuard Extended edition
  AS = VisoGuard Application service edition

  Licensed modules:
  ABS = ABS transcoding for low-bandwidth connections
  LNT = Layout navigation tool
  OPC = iCAT object tracking
  RAO = removed and abandoned object detection
  SB = camera sabotage detection
  SNAP = SNAP (XML integration interface)

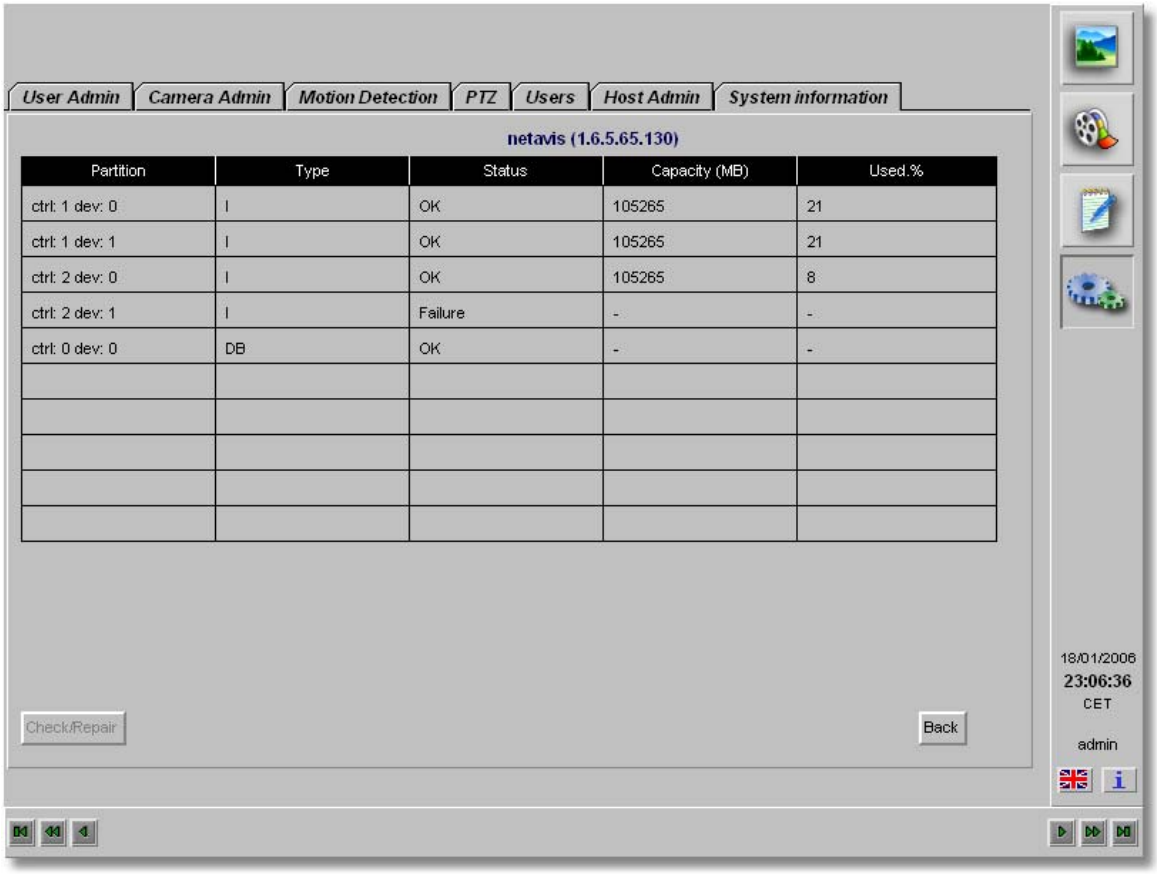
For further information about licensing please refer to the manual *Thecus VisoGuard 4.0 Server Installation and Administration*.

Archive shows the sum of fps and Kbytes per second of archiving on that host.

Monitor shows the sum of fps and Kbytes per second of all logged in users.

Please note that you usually only see the status of your server. If you want to monitor the status of other VisoGuard servers as well, you have to make other servers known to your server (please refer to *11 Working with interconnected VisoGuard servers* on page 79).

2. To show the details of a server, double click an entry or select a server in the table and then choose **Details** from the **System** menu. Now you see detailed information for the selected server:



Here you see the hard disk partitions and their state:

Partition ctrl: shows the number of the hard disk controller; **dev**: shows the hard disk number on the controller. On the screen dump we have 5 disks on 3 controllers.

Type indicates the type of the partition: **DB** is a database holding configuration and event data and **I** is an image partition that holds the actual video image data.

Status indicates whether there is a failure on the partition. Such a failure needs to be reported to your VisoGuard Administrator.

Capacity indicates the size of the partition in MB.

Used % shows how much space of the partition is used.

3. Click on the **Back** button to leave the server details dialog and go back to the list of servers.

10.1.3 Restarting VisoGuard and rebooting the server

1. Choose **System information** from the **System administration** menu. This opens the **System information** dialog.
2. Select a server in the table. In the **System** menu you have the following actions available:

   Stop VisoGuard **system**: This stops all video system processes but does not shut down the server.

   Switch off server: This shuts the server down.

   Reboot server: This reboots the server.

10.2 Setting VisoGuard server parameters

VisoGuard allows you to set several server parameters. To access them, follow these steps:

1. Choose **Host admin** from the **System administration** menu. This opens the **Host admin** dialog.
2. Select your own server indicated by bold face (default is **netavis**). Here you see the Hostname, Network name or IP address and VisoGuard Host ID of your server (are read only). The VisoGuard Host ID is needed for working with distributed VisoGuard server (see next section).
3. Click on the **Next** button. Now you see the Server **Parameters** dialog. Following settings are available:

Field label	Description
Event storage period (days)	Defines how many days events are stored. Any events that are older than these days will be deleted from the event database.
Max number of events stored on server	Defines how many events can be stored in the event database. For each event more than the defined max. number of events the oldest event will be deleted. Please note that both settings, the storage period and the max. number of events, together constrain the event database.
Server timezone abbreviation	Defines the server timezone. Available values are:

Field label	Description
Timeout for IP cameras (sec)	Defines the time after which the message “Camera not responding” appears in the Online Monitor.
Retry count for IP cameras, after which an event is generated	Defines the number of retries after which the server raises a “camera not reachable” event. The **Timeout for IP cameras (sec)** multiplied by this retry count gives the number of seconds, after which an event is generated when an IP camera is unreachable.
Maximum login time for the “guest” user (sec)	Defines the time after which the guest user is forced to logout. If the value is 0, then the guest is never forced to logout.
Timeout for server-server communication (sec)	Defines the time after which an event “Connection lost to server ...” is generated and the cameras mounted from that server disappear from the camera tree (only the root element of the mounted camera tree remains visible, painted in red).
Server network address for camera access	This setting is only important for IP cameras that must actively access the server (e.g. for FTP upload with in-camera motion detection) and only when the server is not accessible by the cameras at its set IP address but at a

Field label	Description
	different address (e.g. due to address mapping). Per default this address always reflects the IP address of the server. You can enter an IP address or a network name.
List of IP addresses from which URL control is enabled	URL control is one way to enable third-party applications to start actions via URL-encoded strings (send http GET request to an VisoGuard server). The server upon receiving these special URL requests converts and executes them as if they would have been generated internally. URL control is only enabled for computers whose IP addresses are entered in this fields (comma separated list). All other requests are blocked. Please refer to the *Release Notes* for further details on URL control.
Transcoding bandwidth limit for live view video streams (kbit/s)	Bandwidth limit per session for transcoded outgoing live view streams. Zero means no transcoding and no limit for live view video streams. Please read *2.5 VisoGuard Transcoding™ for low-bandwidth client-server connections* on page 19 for choosing the best limit values.
Transcoding bandwidth limit for archive playback video streams (kbit/s)	Bandwidth limit per session for transcoded outgoing archive playback streams. Zero means no transcoding and no limit for archive playback streams. Please read *2.5 VisoGuard Transcoding™ for low-bandwidth client-server connections* on page 19 for choosing the best limit values.
Transcoding bandwidth limit for archive export streams (kbit/s)	Bandwidth limit per session for transcoded outgoing archive export streams. Zero means no transcoding and no limit for archive export. Please read *2.5 VisoGuard Transcoding™ for low-bandwidth client-server connections* on page 19 for choosing the best limit values.
IP address of network interface (NIC) for bandwidth limitation	IP address of the network interface (NIC) for which bandwidth limitation is applied. If zero, then the bandwidth limit is applied in total for all available network interfaces. If transcoding is switched on, then it will only be applied to connections of this NIC. If you enter the keyword **NUS** instead of the IP address of the NIC then only traffic to a NUS (VisoGuard user server) is transcoded. Local client connections to this server will not be transcoded. It also works this way if the server has only 1 NIC for all traffic to cameras, local clients and a NUS.
Total outgoing bandwidth limit (kbit/s)	Total bandwidth limit for all outgoing connections of the specified network interface (NIC).
RTSP streaming port	Port number generally used for RTSP communication (e.g. for some MPEG cameras). Please note that modifying the value here does not change the RTSP port setting in the cameras. The cameras need to be configured separately for the RTSP port.
Image database AES encryption (0=no encryption, 1 or	This defines whether the image data are encrypted with

Field label	Description
2=encryption)	AES. Value 0 switches off encryption (default). Entering the value 1 or 2 will switch on AES encryption of the video recording. Value 1 means the system will store the encryption key on a local server disk. Value 2 will store the key on a USB device (formatted with FAT32), which has to be plugged into the server. If the device is not accessible, then archive access is not possible. Prior to inserting the USB device, a writable directory "nek" must me created on the device (this can be done under Windows, for example). VisoGuard will search for this directory and store the key file in it. After the USB device is detected and the key has been written to it the first time, an event with following text is generated: "IDB encryption started, USB device can be removed now for creating backup copy". At this time the USB device can be removed from the server, and a backup copy of the directory "nek" can be created. Note that the stick must be inserted again before any archive query is started.
	Warning: Loss of the encryption key stored on the USB device will make archive access impossible! Also, encryption needs much more CPU power than no encryption (see also *1.3 VisoGuard data security* on page 5).

4. To modify any of these values, select **Modify host** in the menu, set the values and then press **Save**.

11 Working with interconnected VisoGuard servers

VisoGuard allows you to work with the resources of interconnected (remote, distributed) VisoGuard servers. The concept is similar to accessing files on a remote file server. You can import single cameras or whole groups of cameras from other VisoGuard servers and you can also export your locally defined cameras to other VisoGuard servers. You can work with remote cameras as if they would be local (e.g. you can also access their archive, modify their parameters or even add new cameras to remote sites).

Before you can do any of these things, you first have to make both servers known to each other. You can do that by adding the other server as remote server on each of the machines. The next section describes how to do that.

Please note: This chapter just provides a basic introduction to working with interconnected servers. For further details on setting up and administrating a distributed AS system please refer to the manual *Thecus VisoGuard 4.0 Distributed AS Administration*.

11.1 Adding and defining a remote VisoGuard server

1. Choose **Host admin** from the **System administration** menu. This opens the **Host admin** dialog.

   In the menu select **Add host**.

   Fill in the basic information of the desired remote VisoGuard host (server):

Field label	Your input
Hostname	This is the name you give to the remote VisoGuard server. It does not necessarily have to match the actual name of the remote server.
Network name or IP address	This is the network name or IP address of the remote VisoGuard server.
Comment	A descriptive text.
Observer Host ID	This is an internal ID that uniquely identifies the remote server. The ID of an VisoGuard server can be obtained by reading its own entry under the **Host Admin** tab.

2. Now you can define what you want to do with the remote VisoGuard server. Set options according to your requirements:

Field label	Your input
Send local events to remote server	Check this option if you want that your local events are sent to the remote host.
Import of cameras from	Check this option if you want to import cameras from the remote

Field label	Your input
remote server enabled	server.
Export local cameras to remote server	Check this option if you want to export cameras of your server to the remote server. If this option is not enabled the remote server cannot access your cameras.
Monitor remote server status	Check this option if you want to monitor the status of the remote server in **System information** dialog.
Upgrade software on remote server (=upgrade slave)	Check this option if you want to allow automatic distributed software upgrades of the remote server initiated by your current server. In such a case your current local server is the upgrade master and the remote host the upgrade slave. For details about distributed upgrades please refer to the manual *Thecus VisoGuard 4.0 Server Installation and Administration*.
Accept software upgrades from remote server (=upgrade master)	Check this option if you want to accept automatic distributed software upgrades of the current server (=slave) initiated by the remote server (=master). In such a case your current local server is the upgrade slave and the remote host the upgrade master. For details about distributed upgrades please refer to the manual *Thecus VisoGuard 4.0 Server Installation and Administration*.
Request license from remote server (=license master)	Check this option if your current VisoGuard server should check out licenses from the remote server (=license master). For details about floating network licenses please refer to the manual *Thecus VisoGuard 4.0 Server Installation and Administration*.

3. Click on **Save** to save your settings. Now you are ready to import cameras or camera groups from a remote VisoGuard server.

11.2 Working with cameras of another server

In order to work with cameras from another VisoGuard server, following prerequisites must be fulfilled:

- The servers must know each other (see *11.1 Adding and defining a remote VisoGuard server* on page 79)
- The server that exports cameras must have the option **Export local cameras to remote server** set (see *11.1 Adding and defining a remote VisoGuard server* on page 79)
- The server that works with cameras of another server must have the option **Import of cameras from remote server enabled** set (see *11.1 Adding and defining a remote VisoGuard server* on page 79)

After you mount remote cameras you can work with them as if they would be connected to this server. You can access live streaming via the Online Monitor or you can access the archive. If you have the appropriate administrator rights you can also modify camera settings like PTZ, scheduling or motion detection.

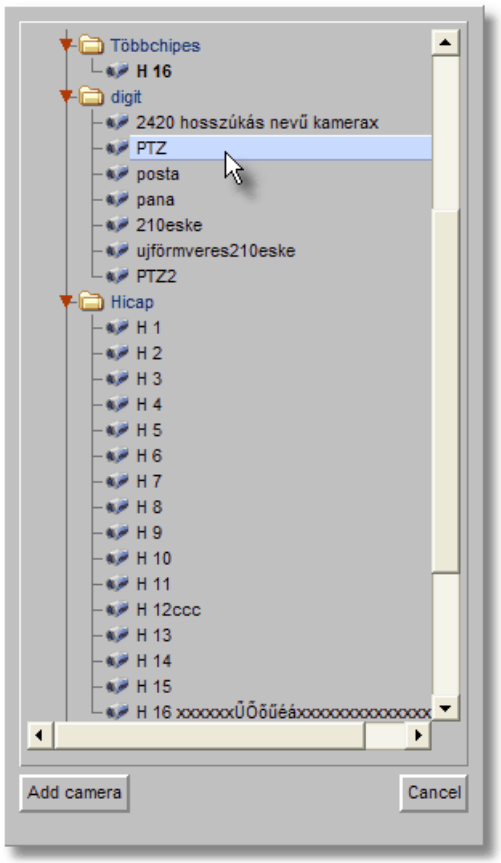
11.2.1 Mounting cameras of another server

1. Choose **Camera admin** from the **System administration** menu. This opens the **Camera admin** dialog.

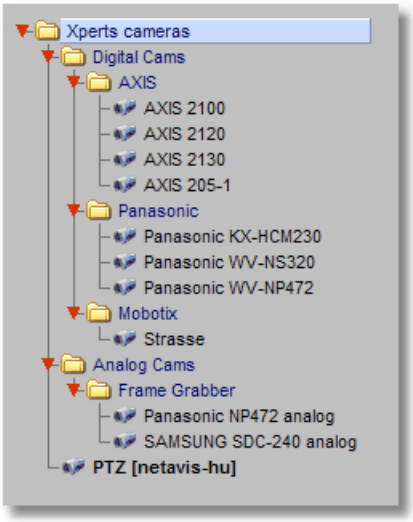
2. In the menu select **Mount remote camera or group**.
3. Select from **Known remote machines** menu item this remote VisoGuard host from where you want to import cameras

   Now the basic data of this remote VisoGuard host are shown again (hostname, IP address).

4. By clicking on **Camera on remote host** selection dialog the whole camera tree from the selected remote host appears and you can select a single camera or group to be imported, e.g. **PTZ** camera on remote host **netavis-hu**.



Confirm your selection by clicking on **Add camera** button.
Now your camera tree shows this imported camera or group in **bold** with the name of the remote server in brackets, e.g. **PTZ [netavis-hu]**.
If the remote server is not reachable, the mounted cameras are not shown in the tree; only the top point of the mounted camera tree appears in red color.



5. With imported cameras you can work the same way as with local cameras. For example, you can display them in a view port in the Monitor (please refer to *5.2 Selecting cameras* on page 35).

11.3 Working with events of remote servers

VisoGuard servers can forward their events to other servers. Such forwarded events are stored in the event database of the generating server itself and also in the event database of the server(s) that receive the events.

Event entries in the event database of remote servers look the same as local events, they just start with the remote server's name and not with the name of the local server. The same kind of search and listing is available as with local events.

In order to receive events from another VisoGuard server, following prerequisites must be fulfilled:

- The servers must know of each other (*11.1 Adding and defining a remote VisoGuard server* on page 79)
- The server that exports events must have the option **Send local events to remote server** set (*11.1 Adding and defining a remote VisoGuard server* on page 79)

11.4 Monitoring remote servers

You can monitor the status of remote servers in the **System information** dialog (see *10.1 Server system information and restarting* on page 72). Before you can do that you have to tell your server to monitor the remote server by checking the option **Monitor remote server status** (see *11.1 Adding and defining a remote VisoGuard server* on page 79).

11.5 Distributed upgrades

When there are several VisoGuard servers in a network upgrading servers to a newer release of VisoGuard one by one can be a very cumbersome and time-consuming task. In order to ease this task, VisoGuard offers an automatic distributed upgrade of all interconnected servers in a network.

Please refer to the manual *Thecus VisoGuard 4.0 Server Installation and Administration* for further details.

12 VisoGuard on mobile devices

You can access an VisoGuard server also from mobile devices like PDAs and mobile phones. This version supports the live viewing of video streams from an VisoGuard server.

This chapter describes how you can install and run VisoGuard on such mobile devices.

12.1 Supported devices

Currently VisoGuard allows you to install the mobile client on these systems:

- Apple iPhone and iPad with OS 3.0 or newer

For further details refer to the VisoGuard start page.

12.2 Installing the VisoGuard client on a mobile device

12.2.1 Apple iPhone

1. Go to the iTunes Store and search for "NETAVIS".
2. Install the VisoGuard application on your iPhone.

12.3 Running the VisoGuard client on a mobile device

12.3.1 Apple iPhone

1. Start the VisoGuard iPhone client.
2. Connect to an VisoGuard server and login.
3. When you get the camera tree tap on a camera to show the live stream.
4. To zoom a camera view in and out in pinch your fingers together or apart. You can also double-tap (tap twice quickly) to zoom in, then double-tap again to zoom out.

13 Working with Layout Navigation

VisoGuard offers powerful layout navigation features that allow you to navigate based on layouts, floor plans, and also other images. In this chapter you learn how to use the layout navigation features.

Please note: Since Layout navigation is licensed separately of VisoGuard you need a valid license in order to work with these features. See also *10.1 Server system information and restarting* on page 72 for details about what license you have.

13.1 Basic concepts and how it works

The VisoGuard layout navigation tool (LNT) allows you to define a hierarchy of **graphical layouts** that correspond to various aspects of your physical environment (section *13.4.1 Planning your layout hierarchy* on page 85 provides details on how to plan the hierarchy).

Layouts that belong together and other related settings can be grouped together in so called **projects**. Depending on the user rights, several users can access and share the same projects and by thus layouts and settings.

On each layout you can place **camera control icons** that correspond to cameras on an VisoGuard server. The camera icons on layouts are interactive, i.e. trigger certain actions when you move the mouse over them or click on them. Such actions can be to show camera live image streams or its recording archive in the corresponding VisoGuard client running on the same client workstation.

On layouts you can also define polygon-shaped **zones** that group certain cameras together and that allow for smart ways of highlighting on events and for good synchronization with the VisoGuard client.

Additionally, you can also display and acknowledge VisoGuard **events** in the tool.

All information used by the LNT (e.g. project and layout definitions, background images, and camera mappings) are stored on the VisoGuard server. Users can use the same LNT information as long as they load the same LNT project, regardless on which client they work.

In a typical installation you would run the VisoGuard client on one screen and the layout navigation tool on another screen (see *2.4 Client multi-window and multi-screen operation* on page 17 for details). However, you can of course run both tools on the same screen as well.

13.2 Installing the layout navigation tool

The layout navigation is available only in the locally installed client which currently runs on MS Windows platforms only (see *2.1 Introduction the VisoGuard client* on page 10).

The Layout Navigation is installed automatically when you install the locally installed VisoGuard client. Please refer to *2.3 Working with the installed VisoGuard client* on page 14.

Note: Currently the layout navigation tool is available only in the locally installed client. For running the layout navigation tool Microsoft .NET 2.0 or a newer version must be installed.

13.3 Starting the layout navigation tool

You can start the layout navigation tool the same way as you can start the installed VisoGuard client. Please refer to *2.3.2 Starting the installed VisoGuard client* on page 14.

The layout navigation tool (LNT) main window looks like this:

13.4 Setting up a project and defining layouts (Editing mode)

In order to setup LNT for work you have to execute a few steps:

- Plan your layout hierarchy
- Select and upload images to be used for layout backgrounds
- Define the hierarchy and map your cameras

In the next subsections we will cover the above topics.

13.4.1 Planning your layout hierarchy

Before you create a project and start to upload graphics images for your layouts it makes sense to plan the layout hierarchy. For example, if your VisoGuard system covers a building then you could have an overview layout image for the building and then separate subordinate layout images for each floor.

For an even bigger setup: If your VisoGuard system covers a whole area with several office or plant buildings then you could have an overview layout image for the whole area and subordinate layout images for each of the buildings and additional images for the parking lots, driveways, fence sectors, etc. Each of the building layouts then in turn could have subordinate layout images for parts of the building like each of the floors. Each of the floors could additionally have subordinate layouts for parts of the floor or even for each of the rooms. Thus you can create hierarchies at arbitrary levels of detail.

13.4.2 Switching to editing mode and creating a project

1. Switch to editing mode by choosing **Project > Switch to editing mode** or by pushing the editing button at the right side of the tool bar.
   In editing mode the LNT window now has added a new control icon list.
2. Create a new project by choosing **Project > New project** and then enter a name of the new project in the newly opened dialog. Push **OK**. Now you start to upload background images for your layouts.

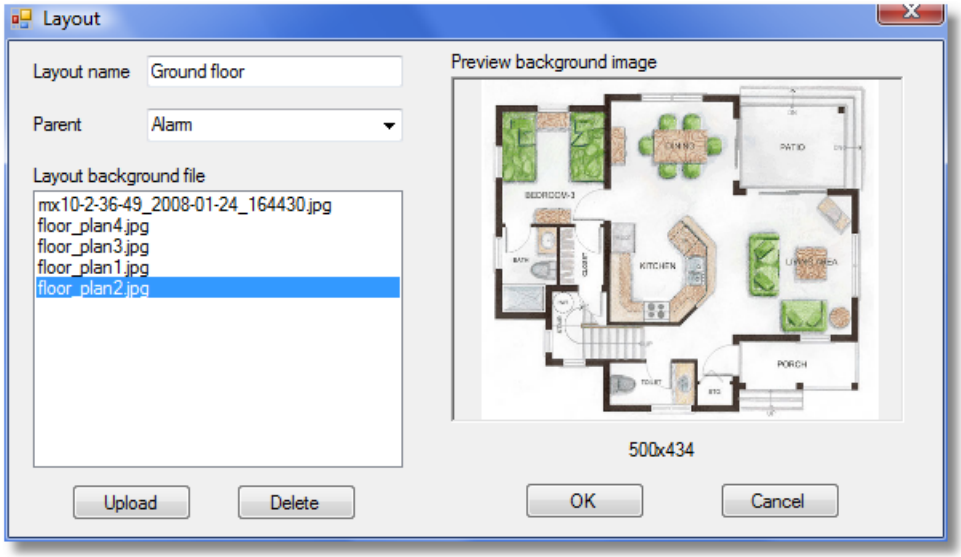
13.4.3 Creating layouts and mapping your cameras

After you planned your layout hierarchy you have to select appropriate images for the various layouts. The layout navigation tool supports popular image graphics file formats like GIF, JPEG, PNG, etc.

Depending on your needs and the available screen resolution for the layout navigation tool (LNT) you have to choose the size (in pixels) for your images. Please keep in mind that the LNT also supports image scaling to fit the available space.

To create a new layout, follow these steps:

1. In the layout navigation tool (LNT) switch to customizing mode by choosing **Project > Switch to editing mode** or by pushing the editing mode button at the right side of the tool bar.
2. In the **Layout** menu choose **New…**, which opens the **Layout** dialog:



3. Enter a name for the layout.
4. Select a background image from the list of available uploaded images or push **Upload** to upload a new background image for the layout (you can also delete uploaded images from the server by selecting an image from the list and pushing **Delete**).
5. If the layout is subordinate to another layout then choose the parent layout from the **Parent** pop-up menu (you can change the layout hierarchy later on via the **Layout > Properties** dialog).
6. Push **OK** to create the layout.
   Now you see that the layout with the selected background image has been created.

Map your cameras

1. From the list of controls at the right side drag a camera control icon with the mouse onto the layout and drop it there. A camera selection dialog opens automatically. Choose the camera and push **OK**. Now you have mapped the camera to your camera icon.

Repeat the above step for other cameras.

You can delete a camera by selecting it with the mouse by choosing **Delete** from the right mouse button pop-up menu.

Defining zones

LNT allows you to group several cameras on a layout into so called zones that can have arbitrary polygon shapes.

Cameras belong to a zone as long as they are positioned inside the boundaries of the zone. You can place an arbitrary number of zones onto a layout.

Here is how you can create a zone:

1. Select a layout from the layout hierarchy.
2. Drag the **Zone field** with the mouse from the controls list at the right side and drop it onto your layout. Where you drop the zone field control with the mouse will be the first corner of the polygon shape and you can now define the zone shape by clicking at further corners. To finish the zone definition, close the polygon shape. Alternatively you can create a rectangular zone by pressing the **CTRL** key while moving the mouse.
3. Per default the zones will be named “Zone-1”, “Zone-2” and so on. You can rename and delete a zone via the right mouse button pop-up menu. Zones can be moved by dragging them with the mouse.

Please note: A zone can trigger certain actions, e.g. when you click with the mouse on it, a zone can show all cameras belonging to the zone in the VisoGuard client. This, for example, will either create a new view in the VisoGuard client or map it to an existing view depending on the names of the views and zones. Therefore the name of a zone can be of importance.
Here is how the mapping works for the LNT action **Show zone live in Observer Client**:
If there is an VisoGuard view that has the same name as the LNT zone and that also contains all the cameras of the LNT zone, then this view is exposed in the VisoGuard client. Otherwise a new view is created with the name of the zone. Details for zone actions can be found under *13.5.3 Modifying zone control appearance and behavior* on page 90.

Linking layouts with link fields

LNT offers link fields to easily navigate between layouts. Link fields can be placed on layouts and are resizable grey areas. Clicking on a link field in Navigation mode will open the “linked” layout.

Here is how you can link layouts via link fields:

1. Drag the **Link field** from the controls list at the right side and drop it onto your layout. Where you drop the zone field control with the mouse will be the first corner of the polygon shape and you can now define its shape by clicking at further corners. To finish the link field definition, close the polygon shape. Alternatively you can create a rectangular link field by pressing the **CTRL** key while moving the mouse.
   After you finished defining the shape of the link field, a dialog is opened offering the available layouts for this link field. Choose a layout by double clicking or by pushing the **Select** button. This defines which layout is to be opened when the link field double clicked in Navigation mode.
2. Choose **Save** from the **Project** menu to save your changes.

Now you can repeat the steps above to create your overall layout hierarchy. You can switch back to Navigation mode by clicking the navigation mode icon at the right side of the tool bar.

Defining a default project

To define a default project to be loaded when LNT is started, follow these steps:

1. In the **Project** menu choose **Set default project…** which opens a dialog listing all available projects. Choose a project and push **Select**. To not load a default project, choose **<No default project>** from the list.

Now this project will be loaded automatically at startup.

Defining a home layout

A home layout can be defined which is automatically shown when the project is loaded. You can set the home layout by following these steps:

1. In the layout hierarchy select the layout that you want to set as home layout.
2. In the **Layout** menu choose **Set as home**.

Now this layout will be opened automatically when the project is loaded.

13.5 Customizing the behavior and appearance of controls

LNT currently has 2 types of controls that can be modified: camera controls and zone controls (the link field control cannot be modified).

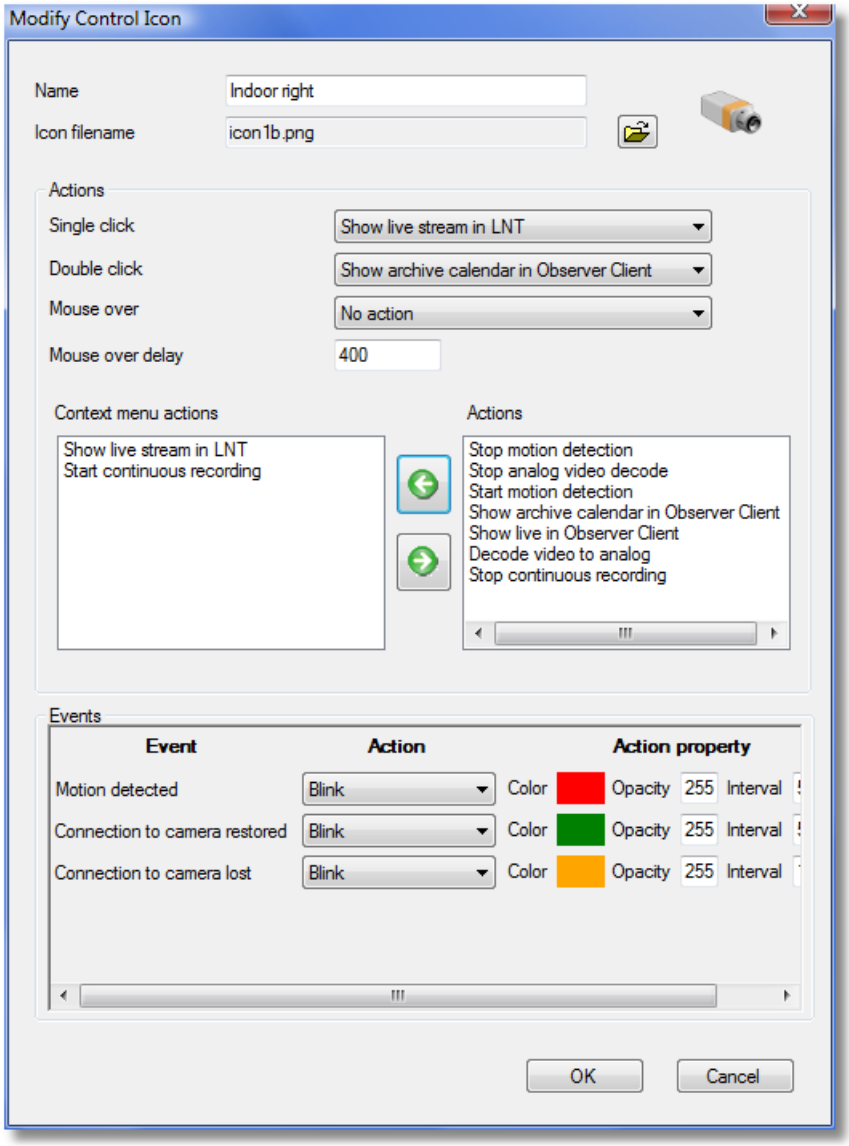
LNT lets you modify several aspects of the appearance and behavior of these control icons:

- Icon image and appearance.
- What happens when you move the mouse over a control icon or when you click on it.
- What happens on certain events originated by VisoGuard related to cameras or zones.

Also you can create new control icons with your own icon images.

13.5.1 Modifying camera control appearance and behavior

1. Switch to editing mode by choosing **Project > Switch to editing mode** or by pushing the editing button at the right side of the tool bar.
2. In the control icon list click on a camera icon with the right mouse button and choose **Modify…** from the pop-up menu. This opens the **Modify control** dialog:



In this dialog you can define the control name and image and which actions are to be performed on certain mouse operations and events.

Actions

The possible **Actions** are:

- **Show live in Observer Client** exposes a large live view of the respective camera in the VisoGuard client that runs on the same machine. If no client is running on the same machine, then noting is happening.
- **Show archive calendar in Observer Client** exposes the archive calendar view of the respective camera in the VisoGuard client that runs on the same machine. If no client is running on the same machine, then noting is happening.
- **Show live stream in LNT** opens a window showing a live stream of respective camera in LNT. If this action is bound to **Mouse over** then the window will be automatically closed when the mouse is moved away from the camera icon. If this action is bound to **Single click** or **Double click**, then the window stays until it is closed manually. To close all such windows, you can select **Close all live streams** in the **View** menu.
- **Start/Stop continuous recording** starts or stops continuous recording of the camera in VisoGuard. It actually sets or deletes the **Enable interval** checkbox in the camera admin's **Scheduling** dialog. Please be aware that there must be at least one continuous recording

interval for the camera for this to work (refer to *6.1.1 Programming continuous timed recordings* on page 43 for details).

- **Start/Stop motion detection** enables or disables motion detection of the camera in VisoGuard. It actually marks or unmarks the **Enabled** checkbox in the camera admin's Motion detection dialog. Please be aware that there must be at least one detection field definition for the camera for this to work (refer to *7.1.2 Basic configuration of server-based motion detection* on page 56 for details).
- **Start/Stop analog video decode** allows the control of special devices that decode IP-based network video signals to analog video signals. This is useful for example for security center video walls that are driven by analog video signals. The configuration of these special devices must be done in configuration files (please refer to the Release Notes or to the customization documentation).

Events

You can also modify the behavior of control icons for certain events, like **Connection to camera lost** or **Motion detected**.

3. Click **OK** to save changes.

13.5.2 Adding a new camera control

1. Switch to customizing mode by choosing **Project > Switch to editing mode** or by pushing the customize button at the right side of the tool bar.
2. In the control icon list click the right mouse button and choose **Add control…** from the pop-up menu. This opens the **Add new control icon** dialog which is essentially the same as the **Modify control icon** dialog above.

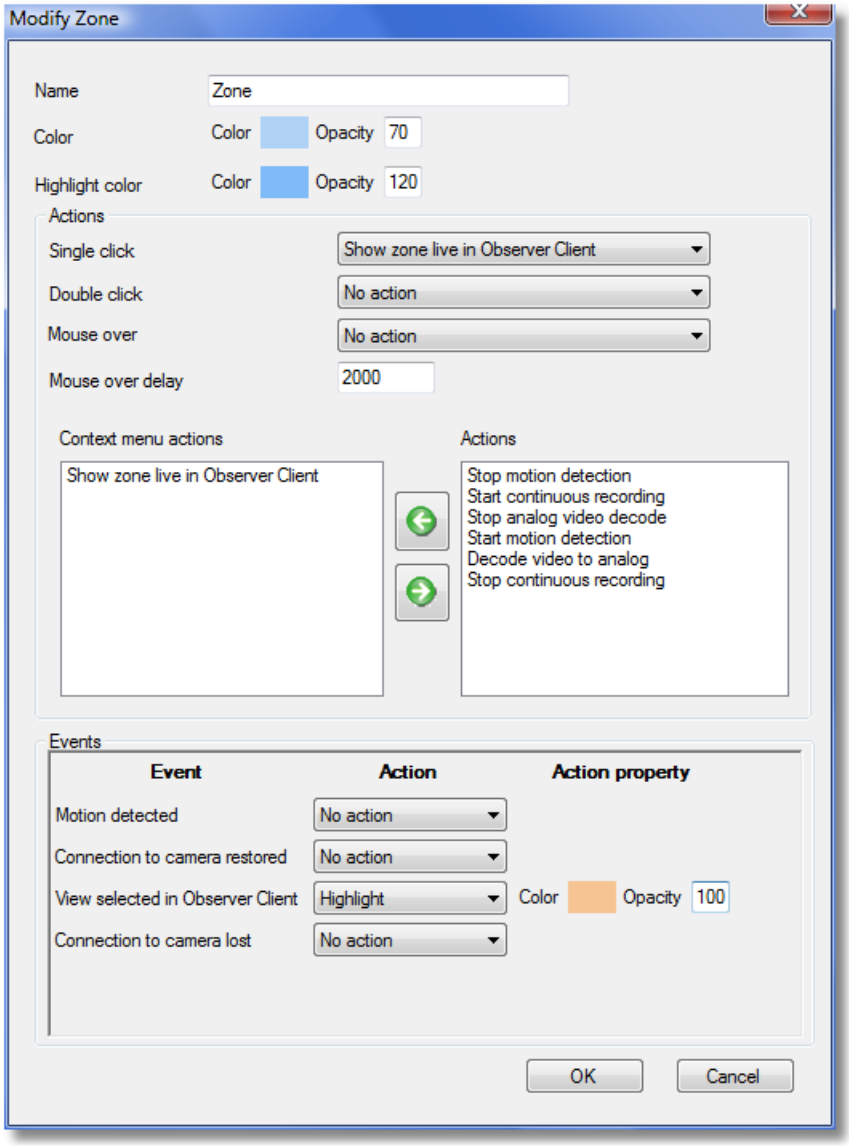
   Here you can define the icon name and image and which actions are to be performed on certain mouse operations.

   You can also modify the behavior for certain events, like color and blinking.

3. Click **OK** to create the new camera control icon.

13.5.3 Modifying zone control appearance and behavior

1. Switch to editing mode by choosing **Project** > **Switch to editing mode** or by pushing the editing button at the right side of the tool bar.
2. In the control icon list click on a zone icon with the right mouse button and choose **Modify…** from the pop-up menu. This opens the **Modify Zone** dialog:



In this dialog you can define the color of the zone and which actions are to be performed on certain mouse operations and events.

Actions

The possible **Actions** are basically the same as for the camera control (see *13.5.1 Modifying camera control appearance and behavior* on page 88) with one addition:

- **Show zone live in Observer Client** exposes the corresponding view of the zone in the VisoGuard client that runs on the same machine. If there is an VisoGuard view that has the same name as the LNT zone and that also contains all the cameras of the zone, then this view is exposed in the VisoGuard client. Otherwise a new view is created with the name of the zone.

Events

You can also modify the behavior of zones of this type for certain events, like **Connection to camera lost** or **Motion detected**.

The event **View selected in Observer Client** works this way: If there is an LNT zone with the same name as the view in VisoGuard then the corresponding action is triggered.

3. Click **OK** to save changes.

13.5.4 Adding a new zone control

1. Switch to customizing mode by choosing **Project > Editing mode** or by pushing the customize button at the right side of the tool bar.
2. In the control icon list click the right mouse button and choose **Add zone…** from the pop-up menu. This opens the **New zone** dialog which is essentially the same as the **Modify Zone** dialog above (see there for details).
3. Click **OK** to create the new zone control.

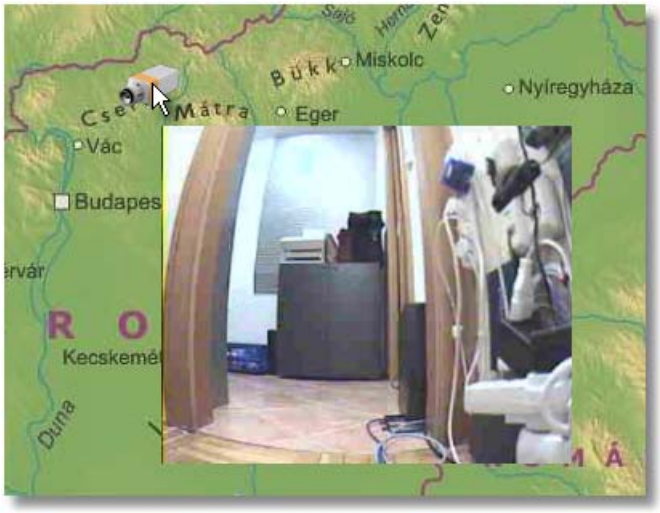
13.6 Layout navigation and operation (Navigation mode)

Switch to Navigation mode by clicking the navigation mode icon at the right side of the tool bar or by choosing **Project > Switch to navigation mode**.

Please note: An VisoGuard client must be running under the same user on the same client workstation so that it can be controlled by the layout navigation tool.

13.6.1 Peeking live video of mapped cameras

The default behavior of some camera icons is that you can peek at live video of mapped cameras by moving the mouse pointer over a camera icon. Then the live video stream will be shown on top of the layout:



As soon as you move the mouse pointer away from the icon, the stream disappears. This behavior can be changed with the **Modify control icon** dialog (see *13.5.1 Modifying camera control appearance and behavior* on page 88).

13.6.2 Showing a camera in the VisoGuard client

When you **single click** a camera icon in LNT then the corresponding camera will be shown in full size in the VisoGuard client. This behavior can be changed with the **Modify control icon** dialog (see *13.5.1 Modifying camera control appearance and behavior* on page 88).
Please note that the VisoGuard client has to be running on the same machine being connected to the same server in order for the feature to work (the client will not be started automatically by LNT).

13.6.3 Positioning to the camera recording archive in the VisoGuard client

When you **double click** a camera icon in LNT then recording archive of the corresponding camera will be shown in the VisoGuard client running on the same machine. This behavior can be changed with

the **Modify control icon** dialog (see *13.5.1 Modifying camera control appearance and behavior* on page 88).
Please note that the VisoGuard client has to be running on the same machine being connected to the same server in order for the feature to work (the client will not be started automatically by LNT).

13.6.4 Navigating in the layout hierarchy

You can position to a layout by clicking its name in the layout hierarchy.

You can also jump to a connected layout by clicking a link field.

13.6.5 Working with events in the layout navigation tool

The layout navigation tool (LNT) also allows you to view and acknowledge VisoGuard events.

Please note: Event handling will only work if the user has the rights to work with events.

When a new event occurs in VisoGuard, then it is displayed in the **Event list** at the right side of the LNT window (the **Event list** can be switched on and off in editing mode by choosing **View > Event list**).

The Project settings define what happens when a new event is coming in (see *13.6.7 Project settings* on page 94): The layout that contains the primary control for related to the event can be exposed automatically and also the control that is related to the event can be highlighted (blinking rectangle).

Additionally a longer description is displayed in the **Event description** field at the bottom of the window (which also can be switched on and off in **Editing** mode by choosing **View > Event description**).

You can acknowledge an event by pushing **Acknowledge** in the Event description field. Acknowledged events will be removed from the Event list. Pressing **Cancel** sets the state of the event to seen (visited) but does not acknowledge it.

Please note that for each camera, a primary control can be defined that is exposed when a new event is generated. You can set the primary flag for a camera icon by right-clicking on the icon in editing mode and choosing **Primary** from the pop-up menu.

Generally, events in LNT can have the following states (indicated by different colors of the event entry):

- New (unseen) events are shown as grey (if it is selected then it is shown in green).
- Seen (visited) events are shown in blue.
- Acknowledged events are removed from the list.

When there are several new events, then LNT offers you to see (visit) them one by one. The exact behavior of the visiting and how the event state can be set to seen (visited) can be defined in the Project settings (see *13.6.7 Project settings* on page 94). You can, for example, mark a new event as seen and jump to the next event by moving the mouse over the blinking control.

13.6.6 Camera status display

LNT allows you to display certain states of cameras in the mapped camera and zone control icons. Examples for states that can be displayed are recording, motion detection active, broken connections, etc.

An example of a status display is:

This camera currently is recording and has motion detection enabled.

To modify the status display settings, follow these steps:

1. Switch to editing mode by choosing **Project > Switch to editing mode** or by pushing the customize button at the right side of the tool bar.
2. Choose **Project > Camera status display settings…** which opens the **Status display settings** dialog.
   This dialog now allows you to define the status settings for camera and zone controls. You can modify the status display settings according to your needs. You can also enable/disable certain status displays by setting the **Enabled** flag.
3. Push **OK** to save your changes or **Cancel** to discard them.

When you switch to navigation mode, the new settings become effective.

13.6.7 Project settings

The layout navigation tool (LNT) allows you to set several project settings that define the workings of the tool. In the **Project** menu choose **Project settings…** to open the **Project settings** dialog.

Here you can set the following values:

Setting	Description
Show home layout on load	Defines whether the Home layout is shown when the tool is started. In order for that to work you must have a home layout defined.
Highlight zone under mouse cursor	Defines whether zones will be highlighted when you move the mouse over them. This can be useful for distinguishing when the mouse cursor is over the zone or over the camera control icon on top of the zone.
Automatically jump to layout on event	In case of an event this setting defines whether the layout that contains the primary control related to the event should be exposed.
Visiting order of events	Defines in which order new events are to be visited.
Set event state to seen (visited) by	When a new event comes in or an existing event is selected, the related control blinks or is highlighted. This setting defines with what mouse operation the state of the event can be set to seen (visited) (blinking is stopped).
Only suggest events of mapped images for visiting	If this checkbox is marked then only events of mapped cameras will be suggested for automatic visiting. If it is unchecked then all events will be suggested.
Standard view size for layouts	Defines the default image size, either **Fit image** or **Full size**.
Event list insertion mode	Defines whether new events in the Event list are inserted from the **Top** or from the **Bottom**.

14 Video analytics with iCAT

iCAT is the video analytics toolkit of VisoGuard. It provides powerful and easy-to-configure object detection and tracking mechanisms as well as a statistics module with integration to the event management system EMS.

iCAT can also interface to 3rd-party video analysis toolkits and algorithms (contact Thecus Technology Corporation).

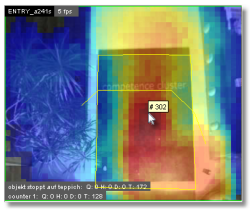
Please note: Since iCAT and some functions are licensed separately of VisoGuard you need a valid license in order to work with these features. See also *10.1 Server system information and restarting* on page 72 for details about what license you have.

14.1 iCAT highlights

- iCAT **works with any camera** that can deliver an MJPEG stream (this covers also analog cameras that are connected via a video server or directly connected to a video grabber card in the VisoGuard server).
- iCAT is **easy to configure** and setup and it **works in difficult situations** also with extreme camera perspectives.
- It offers **flexible scheduling** of iCAT definitions depending on date and time. Thus you can have different setups for weekdays and weekend as well as day and night.
- The **Smart Tripwire™** function for **people and object counting** prevents wrong and double counting and works even with the most difficult entrance situations.

- The Smart Tripwire™ also allows **detecting wrong direction** movements of people and objects.
- **Powerful and robust object tracking** and **event triggering** can be constraint to **object sizes**, **speeds**, and other properties.

- The **Visual Statistics™** module allows you to view various object statistics in an intuitive way.



- Event statistics can be **exported to Excel** XLS for further processing.
- All iCAT detection annotations are **available for live streams and in archived recordings**.

- **Seamless integration** with the VisoGuard event management system EMS and other VisoGuard functions. Additionally iCAT offers **camera sabotage detection** and **lighting change detection**.
- iCAT algorithms have been tuned for the **highest performance** and **least burden on the server**.

14.2 Basic iCAT concepts

iCAT basically consists of the following components that are tightly integrated with VisoGuard:

1. An object detection engine that analyzes the video stream and detects and tracks objects. Please be aware that only moving objects are detected and tracked.
2. An object tracking engine with configurable event triggers decides when a tracked object triggers an event.
3. A real-time statistics module stores statistical information about various aspects of objects like object sizes and speeds.

For setting up a camera with iCAT you essentially configure the following things:

Object tracking region:
The object tracking region defines the part of the camera view in which iCAT is detecting and tracking objects. For each camera you can define one tracking region that is either the full camera view or a part of it in the form of a polygon or rectangle. No object will be detected or tracked outside of this tracking region. Since the CPU overhead caused by iCAT is directly proportional to the size (area) of all the active tracking regions of all active cameras of a server, optimizing the tracking regions will save CPU power.
For each tracking region you can also define what object statistics should be measured by iCAT. Such statistics can then be visualized.

Event triggers: Each camera can have several event triggers that define under what conditions an event is generated by the detected objects. Event triggers only work inside of the object tracking region. Examples of event triggers are people or object counters and detectors of stopped or started objects. The CPU load caused by event triggers compared to the tracking region is negligible.

Scheduling: The standard VisoGuard scheduling mechanisms are also used for scheduling (activating) various iCAT setups. For example, it is possible to have different iCAT settings for weekdays and weekends.

14.2.1 Considerations for setting up a system with iCAT

Camera placement

Generally the iCAT algorithms work with in- and outdoor cameras as well as for different perspectives. The configuration of the algorithms in VisoGuard is pretty simple, as you will see below.

For people and object counting, the best results are possible if the camera is mounted overhead downward looking.

Please note: Setting up iCAT definitions for PTZ cameras is problematic since most of the iCAT functions require a fixed camera position.

Video streams and formats

iCAT works with any video camera. If the camera can provide an MJPEG stream, iCAT uses this format because it is the most efficient for video analytics. If the camera provides only MPEG formats (MPEG-4, H.264, and MxPEG) then iCAT can also work on these streaming formats. However, please be aware that video analytics in MPEG streams requires a lot more CPU power than in MJPEG streams since the decoding is much more complex (for multi-stream operation please see below). Also

video analytics in MPEG streams causes additional delays because it works on groups of pictures or frames (so called GOPs). As a rule of thumb, iCAT adds a delay of approximately 1 GOP duration. Depending on the actual MPEG cameras model, A GOP duration is between 0.5 and 1 sec (see also *3.2 Adding a new camera and setting basic properties* on page 20).

Analog cameras that are connected either via video server or directly connected to an VisoGuard server with a grabber card installed are also supported, of course.

iCAT generally works on CIF (or QVGA or nearest) resolution. This is a good balance between accuracy and CPU overhead. If there is a continuous recording enabled for the camera, iCAT uses this stream for its algorithms and does not cause additional bandwidth. If the size of the stream is bigger than CIF, iCAT downscales it to CIF (or QVGA or nearest) resolution.
Any pixel measures that are available in iCAT are relative to this resolution.

Future releases will also allow you to select higher resolutions for the iCAT algorithms.

CPU load of iCAT (performance issues)

iCAT runs on the server and works very efficiently. The CPU overhead caused by iCAT is directly proportional to the following aspects (see also *14.2 Basic iCAT concepts* on page 97):

- The size (area) of all the active tracking regions of all cameras of a server. This means that optimizing the tracking regions will save CPU power. The number and shape of event triggers is negligible.
- The video processing speed (in fps) of iCAT.
- The streaming format (see above)

An VisoGuard server running with iCAT on standard (not high-end) desktop server hardware can easily handle approximately 10 iCAT-enabled cameras with standard settings.

Additional CPU power (like quad core), enhanced RAM speed, and bigger L2 caches help to boost the iCAT performance.

Multi-streaming operation with iCAT

As indicated above iCAT normally needs much more CPU power for processing MPEG streams (MPEG-4, H.264, and MxPEG) than for processing MJPEG streams. Therefore VisoGuard can pull two parallel streams from the camera if the camera supports that: one MPEG stream for live viewing and recording and 1 additional MJPEG stream for iCAT operation.

In the **Default settings** dialog in **Camera Admin** the checkbox **Multi-stream allowed** enables or disable this dual-stream iCAT processing (see also *3.2 Adding a new camera and setting basic properties* on page 20).

If this checkbox is selected and live viewing or recording is active with an MPEG stream with a frame rate of more than 5 fps or a resolution bigger than VGA 640x480 pixels then VisoGuard will try pull a second MJPEG stream in QVGA fine from the camera for iCAT processing (please note that this stream will be pulled even if the checkbox **Allow JPEG streaming** is deselected). The frame rate of this second stream depends on the iCAT function.

Please note: Dual-streaming iCAT processing will not be activated automatically after selecting the Multi-stream checkboxes. Please restart the server or stop and start (disable/enable) all iCAT functions of the camera in order to activate dual-streaming iCAT after changing the Multi-stream selections.

Object detection

Depending on the sensibility and other settings iCAT currently detects objects of 8x8 pixels or bigger in size. Only moving objects are detected. New objects are detected by iCAT after a few video frames. How quickly objects are detected is also influenced by the sensibility setting.

iCAT video processing speed

If the objects you want to track move very quickly across your camera view you will require a higher video processing speed of iCAT than if they move slowly across your camera view.

Please note: Not the absolute speed of the objects influences what processing speed you need but the relative speed that these objects have in your camera view. This relative speed is influenced by the camera perspective and distance from objects.
Example: Cars on a highway are moving very fast. However if you look at them with a camera from a larger distance and from a perspective with a flat angle the cars are actually are moving pretty slowly in your camera's view. Therefore you can choose a slower video processing speed even for such fast objects like cars on a highway.

14.3 Setting up a camera for video analytics with iCAT

14.3.1 Defining an object tracking region

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Select a camera in the camera tree and in the menu select **Add new definition**.
3. In the **Type** pop-up menu choose **Object tracking region**.
4. In the **Identifier** text field enter a name for this region.
5. Choose whether you want a **Polygon** or **Rectangle** shape by checking the respective check box.
6. Now you can draw the region with the mouse in the preview pane. For a polygon you just click with the mouse to define the corners of the polygon. You close the polygon by crossing an existing edge or by double clicking with the mouse. Here is an example of a tracking region:

Please note: As indicated in *14.2 Basic iCAT concepts* on page 97 and *14.2.1 Considerations for setting up a system with iCAT* on page 97 objects will only be detected and tracked inside a tracking region. Event triggers will only work inside the boundaries of tracking regions. On the other hand, making the object tracking region as small as possible helps you to save CPU power of your VisoGuard server.
Also be aware that the tracking region should approximately at least be twice the size of the biggest objects you want to track.

7. Now you have to set the configuration parameters of the tracking region:

Field label	Your input
Indoor camera	Enable this setting if the camera is an indoor camera. Indoor setting usually is best for rooms not bigger than 10x10m and objects not farther away than 15m. Disable this check box for outdoor environments. Experiment with this setting, if the detection/tracking quality is not ideal.
Overhead downward looking	Enable this setting if the camera is overhead mounted and downward looking. This will improve object separation and the accuracy of object counting. In our example above, the camera is an indoor camera and mounted overhead downward looking.
Sensitivity	Usually this setting should be left at **Normal**. Only if you are not satisfied with the object detection quality or behavior you can try to modify this setting. If you want a sharper object detection and separation, you can set the **Sensitivity** to **High** or **Very high**. Also for example, if you want to detect very small objects, you can improve the sensitivity. The **Sensitivity** also influences how fast new objects are detected. Higher **Sensibility** means quicker object detection, lower means slower detection. For environments that are very noisy visually and that cause too many objects to be detected, the **Sensitivity** can be set to **Low** or **Very low**.
Max object lifetime (sec)	Defines how long a detected object is tracked before it is dismissed by iCAT (i.e. no longer treated as object but essentially becoming background). After an object is being dismissed by iCAT, if it starts moving again, it will be detected as new object.
Max stopped object lifetime (sec)	Defines how long a detected object that stopped is tracked before it is dismissed by iCAT (i.e. no longer treated as object but essentially becoming background). After an object is being dismissed by iCAT, if it starts moving again, it will be detected as new object.
Video processing (fps)	This defines at what frame rate the iCAT algorithms operate. If the objects you want to track move very quickly across your camera view you want to improve the speed. If they move slowly across the camera view you can decrease the speed. See also *14.2.1 Considerations for setting up a system with iCAT* on page 97.
Tolerance radius for stopped object (pix)	Defines when how much a stopped object may move away from its stopping position before iCAT detects it to move again.

8. Push **Next** to get to the **Statistics** settings for the tracking region. Here you can define what statistics iCAT should collect. Later on these object tracking statistics can be visualized (see *14.4.2 Displaying Visual Statistics*™ on page 114. Currently, the following measurements are available: Object counts, speeds, sizes (also for stopped objects).
9. Push **Save** to create the tracking region. Later on you can modify the tracking region settings.

10. If you did not yet define the scheduling for iCAT activities, then after you save the first iCAT definition for a camera, you will be prompted for whether you want to edit the scheduling now.

    Click on the **Yes** button if you want to configure the scheduling now (refer to section *14.3.9 Scheduling iCAT operation and recording* on page 110 for further information).

    Click on the **No** button if you do not wish to schedule the recording or if you want to do that later.

    Please note:
    - If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually (see *14.3.9 Scheduling iCAT operation and recording* on page 110).
    - If a definition is not assigned to a schedule then it will not be activated and no archive recordings will be made and no events will be generated.

iCAT event settings

You can also specify event-related properties on an iCAT definition:

1. You can also choose a specific **Icon** and **Sound** for the event when it is shown in the event task bar.
2. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event**. Please note that the event priority is a relative priority whereby 100 is the default priority (see also *8 Handling events* on page 61).
3. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).

14.3.2 Defining an event trigger for people and object counting (Smart Tripwire™)

Once you have created a tracking region, you can create an arbitrary number of event triggers inside this tracking region. Event triggers define under what conditions an VisoGuard event is generated by iCAT. Such events can trigger automatic recording and are stored in the normal VisoGuard event database that can be queried and exported.

Currently iCAT supports the following event triggers:

- A Smart Tripwire™ for directional people or object counting. This tripwire is directional, so if you want to count objects in two directions you would create two tripwires.
- A polygon or rectangle that creates an event when an object either crosses the field, stops inside the field or starts moving inside the field.

Here are the steps for creating a counting tripwire:

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Select a camera and in the menu and make sure that you have a suitable tracking region defined that allows for object counting.
3. Select **Add new definition**.
4. In the **Type** pop-up menu choose **Event trigger**, which will expose the configuration settings.
5. Under the camera preview choose the **Tripwire** check box for directional people or object counting.
6. Now you can draw the tripwire line with the mouse in the preview pane. You just click with the mouse to define the corners of the polygon. You finish the line by double clicking with the mouse. Here is an example of a tripwire:

This tripwire triggers a counting event whenever an object moves from the green area across the red tripwire. The tripwire is “smart” as it only counts objects that have first been detected in the green area and move across. It would not count the object if it would first be detected in the non-green area, then moved across the line into the green and then move across the tripwire from the green to the non-green area. It also would not double count an object that would have moved across the line twice.

Hints: To count **incoming and outgoing people or objects** you would create two different tripwires with opposite green areas which would both trigger events.
You can also use the tripwire to **detect objects moving in the wrong direction**.

Please note: As indicated *14.2.1 Considerations for setting up a system with iCAT* on page 97 objects will only be detected after a few frames. Therefore an object can move a bit before it is actually detected as object by iCAT. Therefore it makes sense to have the green area big enough to allow iCAT time for the object detection. If that is not the case it might be possible that quickly moving objects are not detected before they cross the tripwire and therefore would not be counted. The ideal settings depend on viewed (relative) object speed and iCAT video processing frame rate.

7. You can also define when an object is counted by either selecting **Object center point**, **Any point of object**, or **Whole object**.
8. When you push the **Next** button you can define additional constraints for the event creation. You can limit the counting only to certain object sizes, certain aspect ratios, and a certain speed. Currently those measures are definable in pixels (please keep in mind that the resolution iCAT works on is either CIF or QVGA depending on the aspect ratio of the camera). Future releases of iCAT will allow for real world measures.

   Zero values in these fields mean that there is no constraint.

Hint for constraining the object size or speed: The size is the area of the object in pixels and the speed is also measured in pixels per second. To know what object sizes or speeds you want to filter it is helpful to watch a few objects passing the triggers and switch on the object markers. These markers show the size and speed of the object in pixels. These are exactly the same measures that you can use for the trigger. Here is an example of an object marker (Object ID is [10], object size is 9110 pixels, speed is 208 pixels/sec):

The section *14.4.1 Displaying iCAT information in the Online monitor and when playing recordings* on page 113 shows you how to view object markers.

9. In the **Identifier** text field enter a name for this event trigger. An example name for a people counter would be "Entrance 1 incoming".
10. You can also choose a specific **Icon** shown and **Sound** played for the event when it is shown in the Event list. Or you can choose to have no icon or no sound associated with the event.
11. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event** (see *8 Handling events* on page 61 for further details on event priorities).
12. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).
13. Push **Save** to save your definition.

Please note:

- If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually (see *14.3.9 Scheduling iCAT operation and recording* on page 110).
- If a definition is not assigned to a schedule then it will not be activated and no archive recordings will be made and no events will be generated.

iCAT event settings

You can also specify event-related properties on an iCAT definition:

1. You can also choose a specific **Icon** and **Sound** for the event when it is shown in the event task bar.
2. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event**. Please note that the event priority is a relative priority whereby 100 is the default priority (see also *8 Handling events* on page 61).
3. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).

14.3.3 Defining an event trigger for object starting and stopping

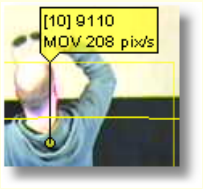
In addition to object counting, iCAT also offers to detect stopping and starting objects in a defined field.

Here are the steps for creating an event trigger for object starting and stopping:

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Select a camera and make sure that you have a suitable object tracking region defined that allows for object counting (see *14.3.1 Defining an object tracking region* on page 99).
3. In the menu select **Add new definition**.
4. In the **Type** pop-up menu choose **Event trigger**, which will expose the configuration settings.
5. Under the camera preview choose the **Rectangle** or **Polygon** check box.
6. Now you can draw the field with the mouse in the preview pane. For a polygon you just click with the mouse to define the corners of the polygon. You close the polygon by crossing an existing edge or by double clicking with the mouse. Here is an example of a tracking region.
7. Now select on what object behavior you want to trigger an event: When an **Object is crossing field**, when an **Object starts moving in field**, or when an **Object stops in field**. You can also define when an event is triggered by either selecting **Object center point**, **Any point of object**, or **Whole object**.

8. In the field **Min. time for stopping, staying inside (sec)** you can enter a minimum time required for an object that either stops or stays inside a field before an event is triggered.
9. When you push the **Next** button you can define additional constraints for the event trigger. You can limit the counting only to certain object sizes, certain aspect ratios, and a certain speed. Currently those measures are definable in pixels (please keep in mind that the resolution iCAT works on is either CIF or QVGA depending on the aspect ratio of the camera). Zero values in these fields mean that there is no constraint.

Hint for constraining the object size or speed: The size is the area of the object in pixels and the speed is also measured in pixels per second. To know what object sizes or speeds you want to filter it is helpful to watch a few objects passing the triggers and switch on the object markers. These markers show the size and speed of the object in pixels. These are exactly the same measures that you can use for the trigger. Here is an example of an object marker (Object ID is [10], object size is 9110 pixels, speed is 208 pixels/sec):



The section *14.4.1 Displaying iCAT information in the Online monitor and when playing recordings* on page 113 shows you how to view object markers.

10. In the **Identifier** text field enter a name for this event trigger.
11. Push **Save** to save your definition.

Please note:
- If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually (see *14.3.9 Scheduling iCAT operation and recording* on page 110).
- If a definition is not assigned to a schedule then it will not be activated and no archive recordings will be made and no events will be generated.

iCAT event settings

You can also specify event-related properties on an iCAT definition:

1. You can also choose a specific **Icon** and **Sound** for the event when it is shown in the event task bar.
2. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event**. Please note that the event priority is a relative priority whereby 100 is the default priority (see also *8 Handling events* on page 61).
3. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).

14.3.4 Defining sabotage detection

iCAT offers intelligent features for detecting three types of camera sabotage actions:

- Camera defocused
- Camera covered
- Camera moved

Please note: For sabotage detection an object tracking region is NOT needed.
When initializing the camera for sabotage detection please make sure that the camera has the correct focus setting and that the scenery and brightness is stable.

Here are the steps for installing an iCAT-based sabotage detection:

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Choose a camera and in the menu select **Add new definition**.
3. In the **Type** pop-up menu choose **Sabotage detection**, which will expose the configuration settings.
4. Select any of the three sabotage detection types.
5. In the **Identifier** text field enter a name for this sabotage detection.
6. Push **Save** to save your definition.

Please note:
- If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually (see *14.3.9 Scheduling iCAT operation and recording* on page 110).
- If a definition is not assigned to a schedule then it will not be activated and no archive recordings will be made and no events will be generated.

Background information on sabotage detection algorithms

Sabotage detection uses three detector algorithms to generate events for camera moved, defocused and covered.

The camera movement detector tries to locate a couple of strong (= has high contrast) points across the entire picture. Then it searches for them on each of the following frames, while continuously creating new points to keep adapting to a new scenery. A "camera moved" event occurs when a given number of these points are lost for a while.

The focus change detector acts like the auto focus algorithms in digital cameras. It estimates the average sharpness of the picture and produces an event if this sharpness changes abruptly. A "focus lost" event is produced if the sharpness of the picture decreases below a threshold, and a "focus gained" event if the sharpness is increased above a threshold. Both thresholds are based on average sharpness values of previous frames.

The camera covered detector uses a brightness analyzer that calculates the average brightness of the picture for each frame and if something strange happens tries to find out what has happened (light switched off, light switched on or just a person in dark clothes passed by). It does so by analyzing a sample of average brightness values collected in previous frames.

The result of the these three detectors are combined to give the final alarm event (camera moved, camera covered, focus lost/gained, brightness change)

Possible reasons of missed or wrong detections

As mentioned above the camera movement detector works with high contrast points on the picture and the focus change detector checks the sharpness of the picture (measuring the sharpness of edges). Logos or date and time text fields generated and placed on the picture by the camera could decrease the accuracy of these detectors or could even prevent detection at all. This is because such overlay fields are always stable, have a high contrast and sharpness and can therefore balance real picture changes, so that the overall change is too small to be detected.

The solution is to either disable these overlay fields in the camera or to mask them out in iCAT (see *14.3.7 Defining a privacy mask* on page 107).

"Focus lost" and "focus gained" events:

A dynamic scene with moving objects of various sizes always changes the average sharpness a little bit and the detector tries to filter out these small variations. This is not always possible, so one can sometimes experience false "focus lost" or a "focus gained" events.

Covering the camera should cause a "camera covered" event, but the effects of the covering could be very similar (from the algorithm's point of view) to a moved camera or to a lost focus. So the algorithm has to decide what happened and the result is not always the proper event category (one may get "camera moved" and more usually "focus lost" instead of "camera covered"). However, a sabotage event should occur at unusual situations, it is just possible that the detailed category will not match the actual reason.

iCAT event settings

You can also specify event-related properties on an iCAT definition:

1. You can also choose a specific **Icon** and **Sound** for the event when it is shown in the event task bar.
2. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event**. Please note that the event priority is a relative priority whereby 100 is the default priority (see also *8 Handling events* on page 61).
3. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).

14.3.5 Defining simple motion detection

Prior to release R1.12 VisoGuard offered simple motion detection only based on a detection of changed pixels between video frames (detection cycles). Simple motion detection does not require an object tracking region.
For more details on setting up and working with this simple motion detection please refer to *7 Working with simple motion detection* on page 56.

14.3.6 Detecting a lighting change

Please follow these steps to enable lighting change detection:

Please note: For lighting change detection an object tracking region is NOT needed.

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Choose a camera and in the menu select **Add new definition**.
3. In the **Type** pop-up menu choose **Lighting change detection**, which will expose the configuration settings.
4. Select the checkboxes for **Light switched on and Light switched off** to detect abrupt lighting changes like when somebody switches the light on or off.

   You can also enter values in the **Brightness high limit (%)** and **Brightness high limit (%)** fields to detect slower lighting changes like during sunrise and sundown. If you leave these values empty, then slower lighting change detection will be disabled.
5. In the **Identifier** text field enter a name for this definition.
6. Push **Save** to save your definition.

Please note:
- If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually (see *14.3.9 Scheduling iCAT operation and recording* on page 110).
- If a definition is not assigned to a schedule then it will not be activated and no archive recordings will be made and no events will be generated.

iCAT event settings

You can also specify event-related properties on an iCAT definition:

1. You can also choose a specific **Icon** and **Sound** for the event when it is shown in the event task bar.
2. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event**. Please note that the event priority is a relative priority whereby 100 is the default priority (see also *8 Handling events* on page 61).
3. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).

14.3.7 Defining a privacy mask

Privacy masks allow hiding private areas of a camera view from live viewing and recording.

This is an example of a privacy mask hiding the text on the carpet:

Here are the steps for creating a privacy mask:

Please note:
- For privacy masking an object tracking region is NOT needed.
- Currently, privacy masks are not shown in exported streams and in the Layout Navigation tool.

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Choose a camera and in the menu select **Add new definition**.
3. In the **Type** pop-up menu choose **Privacy mask**, which will expose the configuration settings.
4. Under the camera preview choose the **Rectangle** or **Polygon** check box.
5. Now you can draw the privacy field with the mouse in the preview pane. For a polygon you just click with the mouse to define the corners of the polygon. You close the polygon by crossing an existing edge or by double clicking with the mouse.

6. In the **Identifier** text field enter a name for this privacy mask.
7. Push **Save** to save your definition.

Please note:
- If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually (see *14.3.9 Scheduling iCAT operation and recording* on page 110).
- If a definition is not assigned to a schedule then it will not be activated and no archive recordings will be made and no events will be generated.

iCAT event settings

You can also specify event-related properties on an iCAT definition:

1. You can also choose a specific **Icon** and **Sound** for the event when it is shown in the event task bar.
2. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event**. Please note that the event priority is a relative priority whereby 100 is the default priority (see also *8 Handling events* on page 61).
3. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).

14.3.8 Defining removed/abandoned object detection

iCAT offers to detect removed and abandoned objects in a defined region.

Please note: For removed/abandoned object detection an object tracking region is NOT needed. Be careful with the size of the region since a greater size will cause a more CPU overhead on the server.

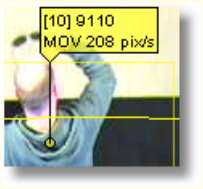
Here are the steps:

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Select a camera and in the menu choose **Add new definition**.
3. In the **Type** pop-up menu choose **Removed/abandoned object**, which will expose the configuration settings.
4. Under the camera preview choose the **Rectangle** or **Polygon** check box.
   Now you can draw the field with the mouse in the preview pane in which you want to detect removed or abandoned objects
   For a polygon you just click with the mouse to define the corners of the polygon. You close the polygon by crossing an existing edge or by double clicking with the mouse. Here is an example of such a field.

Please note: The size of the region for removed/abandoned objects should be at least 20% larger than the objects you want to detect.

5. Select whether you want to **Detect removed objects**, **Detect abandoned objects** or both.
6. In the field **Min. stay time for removed/abandoned objects (sec)** you can enter a minimum time a recognized object must stay, before a remove or abandoned detection on the object and a corresponding event is triggered.
7. In the field **Minimum size removed/abandoned objects (area in pix)** you can constrain the object size for the event trigger. You can limit the counting only to certain object sizes, certain aspect ratios, and a certain speed.
   Currently those measures are definable in pixels (please keep in mind that the resolution iCAT works on is either CIF or QVGA depending on the aspect ratio of the camera). Zero values in these fields mean that there is no constraint.

Hint for constraining the object size: The size is the area of the object in pixels and the speed is also measured in pixels per second. To know what object sizes or speeds you want to filter it is helpful to watch a few objects passing the triggers and switch on the object markers. These markers show the size and speed of the object in pixels. These are exactly the same measures that you can use for the trigger. Here is an example of an object marker (Object ID is [10], object size is 9110 pixels, speed is 208 pixels/sec):



The section *14.4.1 Displaying iCAT information in the Online monitor and when playing recordings* on page 113 shows you how to view object markers.

8. In the **Identifier** text field enter a name for this event trigger.
9. Push **Save** to save your definition.

Please note:
- If you add a new iCAT definition, it will automatically be assigned to all iCAT schedules of the camera. If you do not want that, you have to remove the assignment manually (see *14.3.9 Scheduling iCAT operation and recording* on page 110).
- If a definition is not assigned to a schedule then it will not be activated and no archive recordings will be made and no events will be generated.

iCAT event settings

You can also specify event-related properties on an iCAT definition:

1. You can also choose a specific **Icon** and **Sound** for the event when it is shown in the event task bar.
2. You can also define a special event priority for events generated by the trigger by setting the value **Priority of generated event**. Please note that the event priority is a relative priority whereby 100 is the default priority (see also *8 Handling events* on page 61).
3. The check boxes **Save event in event list** and **Do not save event in event list** allow you to selectively override the general setting for the camera schedule which is defined in *14.3.9 Scheduling iCAT operation and recording* on page 110).

Further considerations and limitations

- Abrupt brightness changes and large variation of white balance (as automatically set by several cameras) may cause false detection, especially false detection of removed objects. In general, if these two conditions become worse, the algorithm become less reliable.
  The best conditions are provided by a stably lit indoor situation. However, the algorithm can also work successfully in outdoor situations. If the lighting conditions are varying heavily, it is recommended to use just abandoned detection (removed detection is switched off), because it is more robust to such varying lighting conditions (through longer detection timeout).
- The region must be carefully defined, i.e. the interesting objects (for example objects of a theft detection) must be fully located inside the region. For example: If you want to detect when your telephone is removed from the table, you can define a relatively small region around the phone to avoid false detections elsewhere, but the region must be a bit larger than the phone allowing the robust detection of its contours. The situation is the same in case of abandoned objects. Abandoned objects which are partially located outside the region may not be detected.
- The objects which are apparently static (stopped person who moved before, person sitting in an office) can also cause false alarms. The detector tries to track moving objects and keep their position when they stop, in order to ignore such objects during detection of really static ones. However through the failures of the tracking such objects may be lost and wrongly classified as an abandoned one. A stopped person who is lost by the tracker becomes the subject of removed/abandoned classification after a given alarm timeout. If it starts moving before the timeout reached, there will be no false alarm raised.
  The possibility of the above mentioned problem increases with the number of person in the scene (as tracker reliability decreases) or with people who only show movement rarely (person working in an office). In the former case you can increase the abandoned detection timeout in order to be more robust, but in the latter one masking out the area where the apparently static person is should be the best.
- There are two alarm timeouts to be set. One for abandoned and one for removed objects. If the scenery is clear, the interesting object is visible then the alarm event will be raised by and large if the timeout is reached. But when another moving or stopped objects (for example the actor itself who is going to leave a luggage) hides or overlaps the interesting object such that it is visible only partially or not at all, the detection time may be longer. So these timeouts are not guaranteed detection timeouts but rather parameters which can increase robustness (setting them longer) or to increase sensitivity (setting them shorter). Of course the alarm event will follow the detection some time around the timeout but the difference depends strongly on the observed scenery.

14.3.9 Scheduling iCAT operation and recording

This section describes how to schedule iCAT video analysis operation and how to define the related event-based recording.

Here are the steps:

1. .

2. In the camera tree select the camera for which you want to program archive recording. Go to the **Scheduling** dialog by clicking on **Next** at the bottom.
3. In the menu select **Modify selected camera or group**.
4. Press the **Add** button below the **Time intervals** list and choose **Video analysis (iCAT)** from the type button labeled **Change**.
5. Now define the days and times when iCAT should be enabled for this camera. You can activate individual days or, with the **All** button, the whole week at once. Select hours and minutes from the time popup.
   Please make sure that the **Enable interval** checkbox is marked, because only then the settings are enabled.

   Note: You can create multiple iCAT intervals for different setups at different times. For each interval proceed as described here.

6. Check the assigned iCAT definitions to this interval via the **Assigned iCAT definitions** popup menu at the right side of the dialog. Per default all available iCAT definitions for this camera are assigned. If you do not want that you can remove them now by deselecting the definition that you do not want in this interval.
7. You can also define whether something should be recorded at an event triggered by one of the assigned iCAT definitions. For that you have a full set of options to set which are described in *6.1.1 Programming continuous timed recordings* on page 43.

   In addition to the parameters for continuous timed recordings you can specify a **Pre-event frame rate (fps)** which can differ from that after the event defined by **Frame rate (fps)**. With **Pre/Post-event recording (sec)** you can specify how long before and after the event you want to record.

   Please note: If there is an active continuous recording in MPEG format, it does not make sense to have any **Pre/post-event recording (sec)** set for the event-based recording. This is because MPEG recording is only done in one quality. See also below for further considerations on pre- and post-event recording.

8. iCAT events for this camera are only stored in the Event database and only appear on the **Taskbar** if the flag **Save event in Event list** is switched on. Otherwise only the recording will start but no event will be stored in the database.
   You can override this setting for individual iCAT events selectively in the corresponding iCAT definition (e.g. *14.3.2 Defining an event trigger for people and object counting (Smart Tripwire™)* on page 101).
9. For all other recording settings please refer to *6.1.1 Programming continuous timed recordings* on page 43.
10. Push **Save**.

    Please note: iCAT-triggered event generation and recording is only active if there is an enabled iCAT interval and there is at least one enabled iCAT definition assigned. Outside of this time interval there is no recording or event generation. Furthermore, recording is started only if either of the fields for **Pre/post-event recording (sec)** is bigger than zero.

Further considerations for pre- and post-event recording

VisoGuard allows you to define the frame rate and quality of event-based recordings. If you want to save video streams for events generated by the video analytics toolkit iCAT please keep in mind that VisoGuard needs to analyze the video stream that it later stores.
Some cameras have limitations when providing multiple video streams at different qualities and frame rates. Therefore VisoGuard tries to retrieve only 1 video stream with 1 quality and frame rate setting whenever possible. This also helps to keep the CPU load for the server and the camera at a minimum.

Here is some information about how event-based recording depending on the video format and pre/post-event frame rate setting is done. This can help you to tune your system to better fit your needs while reducing burden on the server and the camera. For further information on which video

format is best for iCAT please refer also to *14.2.1 Considerations for setting up a system with iCAT* on page 97.

Please note: If the recording event is not generated by iCAT, then the recording behavior is the same as described here, just iCAT is not analyzing the video stream. Simple motion detection involves iCAT. If both, iCAT-based and other event-triggered recording is active at the same time, iCAT recording parameters have priority for obtaining pre-alarm streams.

Event-based recording for iCAT in MJPEG format

- Different frame rates for pre and post event recording

  VisoGuard obtains a QVGA stream for iCAT analyzing and also uses this stream for pre-event recording. In case of an iCAT-based event or alarm, VisoGuard switches to the frame rate and quality defined by the main recording settings (post event).

  Please note: Depending on the camera there can be a small delay caused by the camera needed to switch from the pre-event streaming format to the post-event streaming format.

- The same frame rate for pre and post-event recording

  VisoGuard obtains 1 stream of the main (post-event) recording quality. It also does iCAT analyzing based on this stream (it actually scales the image sizes down to QVGA). In case of an event/alarm, the video stream format is not changed.

  Advantage: same images for pre/post event recordings. No delay between pre- and post-event recording.

  Disadvantage: CPU load is bigger since images need to be scaled down for iCAT analyzing.

Event-based recording for iCAT in MPEG formats (MPEG-4, H.264, and MxPEG)

The majority of MPEG cameras cannot deliver multiple MPEG streams with different formats. Only 1 stream is delivered from the camera. Therefore you need to set the default frame rate to at least the detection frame rate you need for iCAT (see Default settings in *3.2 Adding a new camera and setting basic properties* on page 20).

- There is no pre-event recording (recording time is 0)

  VisoGuard obtains a QVGA MJPEG stream from the camera and runs iCAT analyzing on it. In the case of an event, the streaming format is switched to MPEG and recording is started.

  Advantage: minimal overhead on server CPU.

  Disadvantage: Depending on the camera there can be a small delay caused by the camera needed to switch from the pre-event streaming format MJPEG to the post-event MPEG format.

- There is pre-event recording (recording time is bigger than 0)

  VisoGuard obtains the MPEG stream from the cameras and also does iCAT based on it. Recording is also done with this stream. Please note that iCAT based on MPEG stream needs more CPU power on the server (see also *14.2.1 Considerations for setting up a system with iCAT* on page 97).

Continuous and event-based recording at the same time

If the continuous recording has the same frame rate quality like the post-event recording, then only continuous recording is done and the recording calendar is marked with the events.

If continuous recording is done at a lower frame rate or different quality, then the stream will be restarted with the post-event frame rate und quality in the case of an event.

iCAT processing will be done with continuous recording frames (scaled down in size and/or frame rate if necessary). Pre-alarm setting has no relevance in this case.

14.4 Working with iCAT

In this section you will learn about:

- Watching iCAT information live in the **Online monitor** and also when replaying recordings.
- Displaying Visual Statistics™ in the **Online monitor**.
- Generating reports on iCAT events like people counting and stopped objects.

14.4.1 Displaying iCAT information in the Online monitor and when playing recordings

For each camera that has active iCAT schedules enabled you can display additional iCAT information like object markers and bounding boxes and event trigger fields in the **Online monitor** and also when playing back recordings.

Here is an example of additional iCAT information displayed:

To choose what iCAT information to display you have these options:

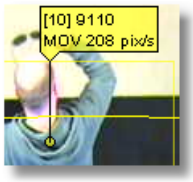
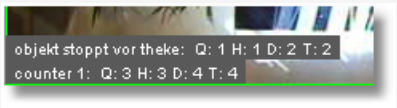
In the **Online monitor** in the view port of a camera that has iCAT processing enabled the view port control menu offers an **iCAT info display** menu (for setting the display for all view ports in a view the same menu is also available via the View control menu **Set parameters of all view ports**).

Also in the **Archive player** you also have an iCAT button with the same menu.

The **iCAT info display** menu allows you to select from various display options: For each of these options you can select **Show always**, **Show on mouse over**, and **Do not show**. For some you also can select **Show on event**.

The display options are:

Tracking boundaries	defines whether the object tracking region boundaries should be shown.
Event trigger lines/boxes	defines whether the event triggers like tripwires and object starting/stopping fields should be shown.
Object markers	defines whether object markers should be displayed. Object markers show the object ID and information about the state of the object (MOV = moving, STP = stopped, LOUNGE = move just a little bit), size and speed.

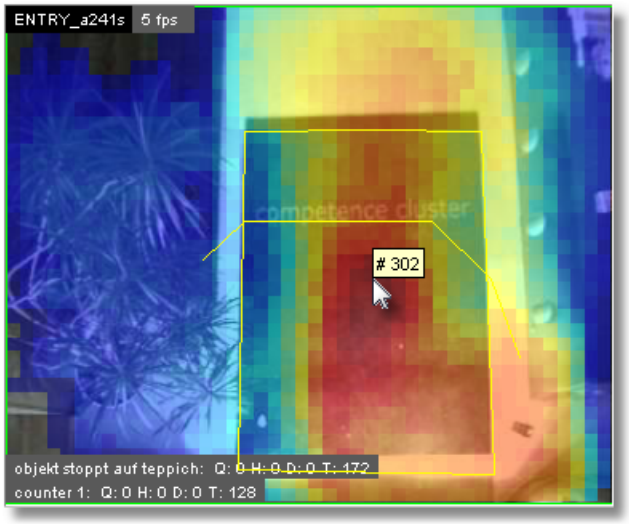
	 In this example object ID is [10], object size is 9110 pixels, and the object is moving with a speed of 208 pixels/sec.
Event count fields	defines whether the event count fields are to be displayed in the lower left corner of the view port. When enabled the count information will be displayed for each event trigger separately in the form of **Q** for last quarter of an hour, **H** for last hour, **D** for day and **T** for total since setup. Here is an example:  There are two event triggers: a field for counting stopped objects and a people counting tripwire (counter 1).
Object bounding boxes	defines whether object bounding boxes should be displayed. Here is an example of an object bounding box displayed: Please note that also the object marker and the event triggers are displayed.

14.4.2 Displaying Visual Statistics™

For each camera that has active iCAT schedules enabled you can display Visual Statistics™ as overlays to the normal video stream in the **Online monitor** and also when playing back recordings.

Please be aware that the statistics are available only inside the object tracking region and that the tracking region must have the collection of statistics enabled (see *14.3.1 Defining an object tracking region* on page 99).

This is an example of visual object count statistics:



To choose what Visual statistics to display you have these options:

In the **Online monitor** in the view port of a camera that has iCAT processing enabled the view port control menu offers a **Visual statistics** menu (for setting the display for all view ports in a view the same menu is also available via the View control menu **Set parameters of all view ports**).

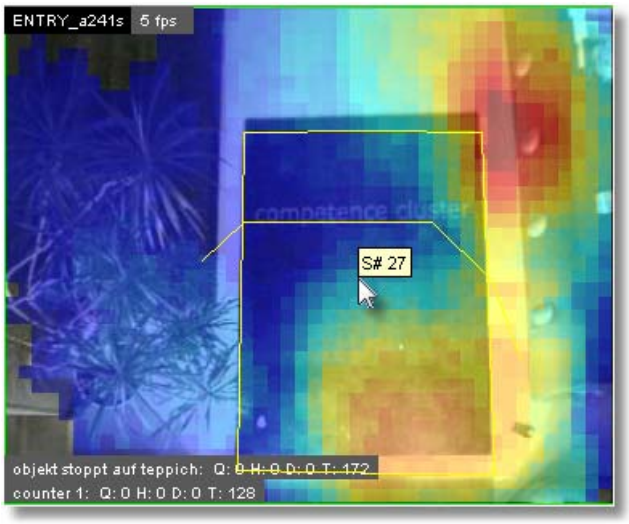
Also in the **Archive player** you also have an iCAT button with the same menu.

The **iCAT video statistics** menu allows you to select the following statistics to display:

For the display of those Visual Statistics you can choose between **Show always**, **Show on mouse over**, and **Do not show**.

In the screen dump above you see an example of the overall object count statistics in an entrance situation. Cold colors mean few object counts and got colors mean high object counts. When you move the mouse over the camera view you can see can see the actual object count for each segment of the view. Above the count in the middle of the screen would be 302 objects.

As a comparison, here you see the Visual Statistics of the stopped object counts of the same camera:



Notice the difference in coloring. You see that people only very seldom stop in the middle of the carpet but stop very often in front of the welcome counter.

Resetting the Visual Statistics

To reset the statistics to zero follow these steps:

1. Choose **Video analysis (iCAT)** from the **System administration** menu. This opens the **Video analysis (iCAT)** dialog.
2. Choose the camera and then the object tracking region.
3. In the menu select **Modify selected definition**.
4. Push the **Next** button to go to the statistics pane.
5. Disable the checkboxes of those statistics you want to reset.
6. Push the **Save** button to save the changes. Now the statistics counts of the disabled statistics are reset.
7. Now enable the statistics again by repeating the above steps accordingly. Do not forget to push **Save** again.

14.4.3 Working with iCAT events

Working with iCAT events is the same as working with other events of the VisoGuard event management system EMS (as described in *8 Handling events* on page 61).

Currently, iCAT generates event of the following types (as shown in the event type hierarchy dialog of the Event search; see *8.1 Event list and event details* on page 61):

Camera specific messages
  State change events
    Video analysis (iCAT) events
      Simple motion detection
      iCAT object tracking

All events that are generated by iCAT (that are not simple motion detection) like people counting, object stopping, and sabotage detection are of type **iCAT Object tracking**. Therefore if you want to filter iCAT events you have to choose the event type **iCAT Object tracking**.

You can differentiate events for the various iCAT event triggers by their names. You can also create event statistics reports in Excel XLS format (see *8.3 Generating an event statistics report* on page 64).

15 Special functions

This chapter describes some special functions of VisoGuard.

15.1 Video annotations

Video streams for live viewing and recording can be annotated with text that then displayed in the video stream. The annotations can come from external data sources and can be stored in the event database for later retrieval and search.

Annotations can be created via the SNAP XML interface or with a simple shell command with command line options.

Example applications are POS cash register data, ATM data, logistics data, or access control data.

15.1.1 Working with video annotations

You can access the video annotation tools from the server's web page:

1. At the server's web page click on **Customizer login** to login to the Customizer area (the admin password is needed for that).
2. After login click on **Download configuration files**.
3. Download the file **annotate.zip** and unpack the zip to a local directory on your client.
4. The zip contains the Windows command line program **annotate.exe**. Just run the program from a command line to see all options. You can also refer to annotate-readme.txt. (The Java source code of the program is also part of the zip file)
5. If you select to generate an event with the video annotation, an event will be stored in the event database for later retrieval and search. By selecting VideoStreamAnnotation in the event type filter of the **Event search** dialog , the annotation text can be searched for by SQL-type wildcards.

15.2 Embedding VisoGuard video streams in web pages

VisoGuard allows you to embed live video streams in standard web pages. Currently only MJPEG stream are supported. The embedding HTML code can be generated by VisoGuard.

15.2.1 Generating the embedding HTML code and testing it

You can generate the embedding HTML code from the server's web page:

1. At the server's web page click on **Customizer login** to login to the Customizer area (the admin password is needed for that).
2. After login click on **Generate embedding HTML code**.
3. Now you can set several options for the embedded applet like size and streaming properties.
4. A click on **Generate applet tag** will open another window that contains the generated HTML code.
5. Push the **Demo** button to run and test the applet in your browser.

16 Index

4

4CIF 8

A

Acknowledging events 62

Active Directory 32

AES encryption of video recordings 77

Annotating videos with data from external sources 116

Anonymize voice 22

Apple iPhone 83

Archive 43

- AES encryption of video recordings 77
- Audio playback 50
- calendar 46
- continuous (timed) 43
- DivX export 52
- event-based recording 45, 109
- exporting 52
- iCAT-based recording 45, 109
- manual recording control in the Online monitor 39
- motion detection in 53
- Playback 46
- programming 43
- protection against deletion 51
- SAFE format export 52
- save space with frame rate reduction for older parts of the archive 45
- storage management 45
- synchronous playback of mutiple cameras 50
- time zoomimg 50

Aspect ratio

- of JPEG images 8, 21
- of Online monitor views 34
- PAL, NTSC, VGA, HDTV 34

Audio

- playback in archive 50
- settings 22
- working with cams 41

AVI

- exporting from archive 52

B

Bandwidth

- limiting overall outgoing bandwidth of server 77
- support for low bandwidth via Transcoding (tm) 19

Brightness 26

C

Calendar in archive 46

Camera

- access rights for users 31
- clone existing camera 26
- default settings 22
- duplicate existing camera with similar settings 26
- groups 27
- moving in camera tree 28
- multicast streaming for MPEG 22
- port mapping on video server 28
- privacy mask 106
- sabotage detection 103
- setup 20

status display (LNT) 93
video analytics (iCAT) 95
Camera finder in the Online monitor 37
Camera tree
drag and drop cameras 35
how to work with it 35
positioning in the window 18
CIF 8
Client
languages 12
locally installed 14
multi-window/multi-screen operation 17
overview of components 17
starting 10, 14
support for low-bandwidth connections 19
web browser 11
Clone camera 26
Contrast 26
CPU load
and streaming formats 7
display of server CPU load 72
for video analytics (iCAT) 97
Cropped view ports
define which part to display 38

D

Data integration with external applications 116
Data security 5
Default settings
for cameras 22
Deleting windows 18, 19
Demo mode license 10
Distributed upgrades of servers 82
DivX exporting from archive 52
Documentation set 5
Drag and drop
camera from the camera tree to view ports 35

E

Encryption
AES encryption of video recordings 77
general description 5
HTTPS for connection to camera 21
Event
acknowledging 62
Event list
create a separate Event list window 18
maximizing 18
positioning in the window 18
Event triggers (iCAT) 96, 100
Events 61
details 62
Event list 61
modifying layouts 18
priorities 61
sorting 61
event-based recording 109
HTML export 64
in layout navigation 93
priorities 61
remote servers 82
searching in the event database 63
short replay 62
statistics 64
user privileges for accessing and handling 61
video analysis (iCAT) 115
Exiting the client 19
Exporting archive recordings 52

F

Floating window components 18

Four-eyes principle 29
Frame rate
  changing in view port 37
  maximizing 37

H

H.264 6, See also MPEG
HDTV 16/9
  aspect ratio in Online monitor 34
HTML code for embedding streams in web pages 116
HTTPS encryption 21

I

I/O contacts
  settings 25
iCAT 95
  considerations for setting up 96
  CPU load 97
  event triggers 96, 100
  event-based recording 45, 109
  events 115
  object bounding boxes 113
  object counting 100
  object markers 112
  object tracking region 96, 98
  people counting 100
  privacy mask 106
  recording based on 45, 109
  removed/abandoned objects 107
  sabotage detection 103
  scheduling activities 45, 109
  sensitivity setting 99
  Smart Tripwire(tm) 100
  starting and stopping objects 102
  video processing speed 98
  video streaming formats 96
  Visual Statistics™ 113
  working with in Online monitor 112
In-camera motion detection 59
  settings 25
IP address
  of camera 21
iPhone 83

J

Joystick control for PTZ cameras 70
JPEG
  aspect ratio 8, 21
  exporting from archive 52
  image sizes and quality 8
  MJPEG vs. MPEG 6

L

Languages 12
Layout navigation 84
  editing mode 85
  installation 84
  navigation and operation 92
  zones 87
Layout of windows
  modifying 18
LDAP 32
License
  displaying current license 73
  license string 10
Login
  secondary password 29
  the locally installed client 14
  the web-based client 13
Low-bandwidth connections with Transcoding(tm) 19

M

Manual recording control in the Online monitor 39
MJPEG 7
  versus MPEG streaming 7
Mobile devices, PDAs 83
Motion detection 56
  in archive 53
  in-camera 59
  recordings based on 45, 109
  server-based 56
Motion JPEG 7
MPEG 6, 7
  settings 22
  versus MJPEG streaming 7
  working with cams 41
MPEG-4 6, See also MPEG
Multi streaming (parallel video streams) 6
  enabling 22
  optimizing iCAT operation 97
Multicast streaming for MPEG cameras 22
Multi-screen operation 17
  positioning windows 19
Multi-window operation 17
MxPEG 6, See also MPEG

N

NTSC 8

O

Object bounding boxes (iCAT) 113
Object counting (iCAT) 100
Object markers (iCAT) 112
Object tracking region 96
Online monitor 34
  creating views 34
  defining views for new user 31
  manual recording control 39
  navigating in the 36
  quick camera finder 37
  view port quality settings 37
  view settings 37
  working with iCAT 112
  zooming in a view port 38, 49
Overlay painting 17

P

PAL 8
pan, tilt, zoom 66
Password
  changing 32
PDAs (mobile devices) 83
People counting (iCAT) 100
Playback of archive recordings 46
Port mapping
  of analog cameras on video server 28
Priority
  of events 61
  sorting event list 61
Privacy mask (iCAT) 106
Privileges of users 30
Protect archive recordings against deletion 51
PTZ (pan/tilt/zoom) 66
  automatic routes 70
  control with motion detection 58
  controlling camera 67
  joystick control 70
  routes 66
  user priority 30

Q

QCIF 8

Quality settings
changing in view port 37
Quitting the client 19

R

Recording 43, See also Archive
Release notes 5
Remote servers 79
events 82
monitoring 82
upgrading 82
Restarting and rebooting 75
Round tours 40
RTSP streaming port 77

S

Sabotage detection (iCAT) 103
SAFE format archive export 52
Saturation 26
Scheduling
iCAT activities 45, 109
Screen resolution
minimum for running the client 10
Secondary password
for login 29
Security 5
Sensitivity setting (iCAT) 99
Server network 79
Server parameters 75
Servers
administrating 72
information about running 72
load display 72
remote, distributed 79
Smart guard function 40
Smart Tripwire (iCAT) 100
Smartphones (mobile devices) 83
Statistics
events 64
iCAT Visual Statistics™ 113
Storage management in archive 45
Streaming formats 6
changing in view port 37
iCAT video analytics 96
Synchronous playback of mutiple cameras in archive 50

T

Time zone of server 75
Time zoomimg in archive 50
Transcoding (tm) for low-bandwidth connections 19
setting up 77
Tripwire for object counting (iCAT) 100

U

Upgrading
remote servers 82
URL
controlling via URL requests 77
Users
Active Directory/LDAP 32
adding 29
camera access rights 31
copying view between 41
groups 31
info about logged in 31
managing 29
privileges 30

V

VGA 8
Video analytics 95

video annotations 116
Video compression 6
MPEG vs. MJPEG 6
Transcoding for low bandwidth connections 19
View port
define crop view 38
View ports
creating 34
quality settings 37
zooming camera views 38, 49
Views
copying between users 41
Online monitor 34
round tours 40
settings 37
Visual Statistics™ (iCAT) 113

W

Web pages
embedding live video streams 116
Windows
create a separate Event list window 18
deleting 18
modifying layouts 18

Z

Zones in layout navigation (LNT) 87
Zooming
in an Online monitor view port 38, 49
in SAFE exports 53
of PTZ cameras 69